Kaseya 2

Network Monitor

Benutzerhandbuch

Versión R8

Deutsch

January 6, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

©2014 Kaseya. All rights reserved. | www.kaseya.com

Inhalt

Network Monitor Überblick 1

Installation 3

Checkliste vor der Installation....4
Network Monitor Modulvoraussetzungen....4
Server Sizing....4
Installieren einer neuen Instanz von Network Monitor R8....5
Migration von KNM unabhängig zu KNM integriert....6
Übersicht zur Konfiguration....9

Verwaltungsschnittstelle 11

Erste Schritte....13
- Die Monitoring-Ansicht....13
- Monitorstruktur....14
- Vererbung....15
- Navigationsleiste....15
- Listenansichten....15
- Knoten- und Benutzersuche....16
- Listenansichts-Steuerungselemente....17
- Listenansicht filtern....17
- Datenansichten....19
- Eigenschaften und Befehle....20
- Menüs bearbeiten....20
- Verschieben von Knoten....21

VSA-Integration....22
- Überblick über das Navigationsfeld....22
- Integration mit Discovery....23
- Gatewayknoten und Netzwerkermittlung....25
- Installieren und Deinstallieren von Gateways....25
- Unternehmen und Rechnergruppen....26
- Umbenennen von Gateways und Beständen....27
- Ticket-Aktion....28
- Benutzerintegration....28
- Network Monitor Lizensierung in VSA....28

Gateways....29
- Gatewaybefehle und -ansichten....30
  - Registerkarte "Bestand"....31
  - Registerkarte "Monitore"....32
  - Registerkarte "Karte"....32
  - Registerkarte "Toplist"....34
  - Registerkarte "Zeitpläne"....35
  - Registerkarte "Knowledge"....37
  - Registerkarte "Audit"....37
- Bearbeiten von Gateways....37
  - Registerkarte "Basiseigenschaften" – Gateways....38
  - Registerkarte "Erweitert" – Gateways....38
  - Registerkarte "Authentifizierung"....40

Registerkarte "NOC" 41
Untergruppen 42
Gruppenbefehle und Ansichten 44
Hinzufügen / Bearbeiten von Untergruppen 44
Registerkarte "Basiseigenschaften" – Untergruppen 45
Registerkarte "Erweitert" – Gruppen 45
Registerkarte "Markierungen" 46
Bestand 47
Bestandsbefehle und Ansichten 48
Registerkarte "Monitoring" 48
Registerkarte "Statusänderungsprotokoll" 49
Bearbeiten von Beständen 49
Registerkarte "Basiseigenschaften" – Bestand 50
Registerkarte "Erweitert" – Bestand 50
Testen von Abhängigkeiten 52
Bestandsvorlagen 52
Monitore 53
Monitorbefehle und Ansichten 55
Registerkarte "Übersicht" 56
Registerkarte "Aktionen" 56
Registerkarte "Alarm simulieren" 59
Hinzufügen von Monitoren 59
Hinzufügen von vorkonfigurierten Monitoren 60
Bearbeiten von Monitoren 61
Registerkarte "Grundlegend" – Monitore 63
Registerkarte "Erweitert" – Monitore 63
Registerkarte "Alarmfilterung" – Monitore 64
Registerkarte "Statistiken" – Monitore 64
Alarmmeldungen 65
Formatvariablen 66
Bestätigen von Alarmen 68
Berichte 69
Anzeigen von Berichtsvorlagen 70
Schnellberichte anzeigen 71
Anzeigen angepasster Berichte 73
Berichte per E-Mail versenden und veröffentlichen 73
Planen von Berichten 75

Informationen zum Navigationsfeld 77

Überblick über das Navigationsfeld 78
Berichte angepasst 79
Berichtsvorlagen 80
Berichtseigenschaften 81
Berichtstile 81
Berichtsdaten 82
Berichtsdatentypen 82
Diagramme 84
Datentabellen 85
Ausfallzeitbericht 86
Kommentare 87
Abbilder 87
Toplists 88
Knowledge-Base-Artikel 89
Knowledge-Base-Kategorien 91
Dashboard 92

Bestandswartung 93
Bestandswartung bearbeiten 93
Monitorwartung 94
Pflege überwachen bearbeiten 94
Benutzerbenachrichtigungspläne 95
Benutzerarbeitsplan bearbeiten 95
Zeitplanblöcke 96
Liste der Windows-Dienste 96
MIB Browser 97
MIB-Objekte 98
Kompilieren von benutzerdefinierten MIB-Dateien 99
Datensatzmanagerprotokoll 100
Syslog-Meldung 101
Systemadministratorkonsole 102
Systemprotokoll 104
Trap-Meldungen 104
Eigene Einstellungen 104
Registerkarte "Basiseigenschaften" 105
Registerkarte "Benutzeroberflächenoptionen" 105
Benutzerbenachrichtigungsgruppen 105
Eine neue Benutzergruppe erstellen 105
Angepasste Datentypen 106
Bestandsvorlagen 107
Bearbeiten von Bestandsvorlagen 107
Protokolleinstellungen 108
NOC-Einstellungen 109
Weitere Systemeinstellungen 109
SMS-Einstellungen 110
Standardnachrichten 113

Monitorreferenz **115**

Active Directory-Monitor 117
Bandbreitenauslastungsmonitor 118
CIM-Monitor 119
Citrix-Servermonitor 120
CPU-Auslastungsmonitor 120
Datenbankservermonitor 121
Datenspeicherauslastung 122
DHCP-Abfragemonitor 123
Verzeichniseigenschaftsmonitor 123
Plattenauslastungsmonitor 124
DNS-Suchmonitor 125
Umgebungsmonitor 126
Ereignisprotokollmonitor 126
Exchange-Servermonitor 127
Dateiänderungsmonitor 128
FTP-Servermonitor 129
IMAP4-Servermonitor 129
JVM-Systemmonitor 129
LDAP-Abfragemonitor 131
Protokolldateimonitor 131
Lua-Skriptmonitor 132
Mailserver-QOS-Monitor 133
Speicherauslastungsmonitor 133
MySQL-Monitor 134

NNTP-Servermonitor 135
Oracle-Monitor 136
Ping-Monitor 137
POP3-Servermonitor 138
Prozessstatusmonitor 138
Radius-Monitor 139
Salesforce-Abfragemonitor 140
SMTP-Servermonitor 141
SNMP-Monitor 141
SNMP-Trap-Monitor 142
SQL Server-Monitor 143
SSH2-Skriptmonitor 145
SSH2-Servermonitor 145
Auslagerungsdateiauslastungs-Monitor 146
Syslog-Monitor 146
TCP-Port-Scan-Monitor 147
Telnet-Servermonitor 147
Terminaldienstmonitor 148
TFTP-Servermonitor 148
Übertragungsgeschwindigkeitsmonitor 148
VMware-Systemmonitor 149
Webservermonitor 150
Windows-Systemmonitor 151
Windows-Dienststatusmonitor 152
WMI-Abfragemonitor 152

Aktionsreferenz **155**

Aktion "Ereignisprotokoll löschen" 156
Aktion "Befehl über SSH2 ausführen" 156
Aktion "Windows-Befehl ausführen" 157
Aktion "HTTP Get/Post" 157
Aktion "Liste zurücksetzen" 158
Aktion "Lua-Skript" 159
Aktion "E-Mail senden" 159
Aktion "Nachricht über PageGate senden" 160
Aktion "SMS senden" 160
Aktion "Wake-On-LAN-Paket senden" 161
Aktion "SNMP-Set" 161
Ticket-Aktion 162
Aktion "Windows-Dienststeuerung" 163

Informationen zum geplanten Ereignis **163**

Ereignis "Ereignisprotokoll" löschen 163
Ereignis "Befehl über SSH2/Telnet ausführen" 164
Ereignis "Windows-Befehl ausführen" 164
Ereignis "Statistiken exportieren" 165
Ereignis "Bericht generieren" 167
Ereignis "HTTP GET/POST-Anfrage" 168
Ereignis "Lua-Skripte" 169
Ereignis "E-Mail senden" 169
Ereignis "Nachricht über PageGate senden" 170
Ereignis "SMS senden" 170
Ereignis "Wake-On-LAN-Paket senden" 171

Ereignis "SNMP-Set" 171
Ereignis "Monitor auslösen" 172
Ereignis "Windows-Dienststeuerung" 172

Weiterführende Informationen 173

Init.cfg-Parameter 174
Backup und Wiederherstellung 175
Backup von Network Monitor 175
Wiederherstellen der Konfiguration 176
Datenextrahierungsreferenz 176
dir 177
monitor_graph 177
monitor_status_list 177
monitor_statusstring 178
monitor_uptimestring 178
device_xml 179
devicelist_xml 181
user_status 182
test_status 182
Version 183
UNIX-Systemunterstützungsdateien 183
Aktivierung des ODBC-Treibers 185

Windows-Problembehandlung und -Systemmonitor 189

Fehlerbehebung – Windows-Überwachung und -authentifizierung 190
Network Monitor -Dienstkonto und Zuweisung von Rechten 190
Monitore mit Windows-Authentifizierung 190
Ereignisprotokollmonitor 191
Dienstmonitor 191
Externe Ressourcen 191
Fehlerbehebung 192
Zugriff verweigert 192
Netzwerkpfad kann nicht gefunden werden 192
Leistungsprobleme bei überwachten Beständen 193
Der RPC-Server ist nicht verfügbar 193
Windows-Leistungsregistrierung 194
So überprüfen Sie, ob KNM Zugriff auf den Remoteregistrierungsdienst hat 194
Arbeitsspeicherverlust bei Remoteregistrierungsdienst auf überwachtem Rechner 195
Zwischenspeichern von Zählern 195
Windows-Verwaltungsinstrumentation (WMI) 195
Überprüfen, ob WMI für das Konto aktiviert ist 197
Anpassen der Firewall-Einstellungen 199
Zusatz für Benutzer, die nicht Administrator sind 199
Überprüfen, ob WMI funktioniert 199
Vollständiger Index von Artikeln zur Fehlerbehebung bei Microsoft WMI 201

Informationen zu Dienstprogrammen 203

Überblick über Dienstprogramme 204
Kompilieren von benutzerdefinierten MIB-Dateien 204
Lua 205
Gizmo 207
Dashboard Map Editor 208

Starten von Map Editor 209
Importieren von Kartenbildern 210
Konfigurieren von Karten 211
Bearbeiten von Kartenknoten 212
Hinzufügen von Kartenknoten 212
Verwenden der Organisationswerkzeuge 213
Veröffentlichen von Karten 214
Visualisierung der Bandbreiten-Auslastung 214
Erstellen einer Bandbreitenverbindung 215

Inhaltsverzeichnis **217**

Network Monitor Überblick

Network Monitor ist eine web-basierte Monitoringlösung zur Überwachung der Leistung und Verfügbarkeit einer breiten Palette von Netzwerkbeständen. **Network Monitor**Monitoring findet *ohne Agents* statt, was bedeutet, dass keine Software oder Dateien auf überwachten Rechner installiert werden. **Network Monitor**bietet mehr als 40 integrierte Monitoringmethoden. Diese Methoden können mit Lua-Skripten erweitert werden. Erweiterte **Network Monitor**-Merkmale umfassen mehrstufige Alarm-Eskalationen sowie die Fähigkeit, Alarm-Abhängigkeiten zu konfigurieren, sodass Service-Anbieter lediglich die wichtigsten Alarme erhalten. Es werden alle gängigen Betriebssysteme unterstützt, einschließlich:

- AIX (4.2 und darüber)
- CentOS
- Debian
- Fedora
- FreeBSD
- HP-UX
- Generic Linux
- OpenBSD
- OpenSUSE 10.2
- Red Hat Enterprise Server
- Solaris
- Ubuntu
- Fenster

Konditionen und Konzepte

- **Bestand** – Ein Bestand repräsentiert einen Computer oder eine andere Art Netzwerk-Gerät, das *durch eine IP-Nummer oder einen Hostnamen bezeichnet werden kann*. Ein Bestand enthält Einstellungen, die für alle Monitore gleich sind, die mit diesem Bestand verbunden sind.
- **Monitor** – Ein Monitor prüft eine bestimmte Funktion in einem Bestand. Die meisten Monitore sind in der Lage, mehrere statistische Daten zu Berichtszwecken zu sammeln. Wenn ein Monitortest nacheinander eine bestimmte Anzahl von Ausfällen aufweist, geht der Monitor in einen *Alarmstatus* über und führt eine Reihe von Aktionen durch.
- **Untergruppe** – Eine Untergruppe ist ein "Container-Knoten" für andere Knoten in der **Network Monitor**-Monitorstruktur. Normalerweise repräsentieren Untergruppen einen logischen Geschäftsbereich.
- **Aktionen** – Eine oder mehrere Aktionen können ausgeführt werden, wenn ein Monitor eine bestimmte Anzahl nacheinander durchgeführter Tests nicht besteht. Eine Reihe von Wiederherstellungsaktionen kann ausgeführt werden, wenn ein Monitor nach einem *Alarmstatus* wiederhergestellt wird.
- **Bestandsvorlage** – Eine Bestandsvorlage wird verwendet, um Beständen eine Reihe an Monitoren zuzuweisen. Sobald Beständen einer Bestandsvorlage zugewiesen wurde, werden Änderungen an den Bestandsvorlagen auf alle zugehörigen Bestände übertragen.
- **Benutzergruppe** – Bei einer **Network Monitor**-Benutzergruppe handelt es sich um eine Reihe an VSA-Benutzern, die benachrichtigt oder geplant werden können, um für eine Benachrichtigung verfügbar zu sein. Jeder Bestand in **Network Monitor** ist einer Benutzergruppe zugewiesen. Wenn ein Monitor in einen *Alarmstatus* übergeht, werden Benachrichtigungen normalerweise an die Benutzergruppe des Bestands gesendet.

- **Anmeldedaten** – Bei den Anmeldedaten handelt es sich um einen Benutzernamen und Passwort, die den Zugriff auf eine Ressource autorisieren. **Network Monitor**speichert Anmeldedaten getrennt vom Rest von VSA. Diese Anmeldedaten werden von Monitoren, Aktionen und Ereignissen verwendet, um Zugriff auf die entsprechenden Ressourcen zu ermöglichen, wenn ein Vorgang durchgeführt wird.

Statussymbole

Ein Monitor befindet sich immer in einem bestimmten Status. Dieser Status wird in der **Network Monitor**-Benutzeroberfläche durch unterschiedliche Farben veranschaulicht. Ein Bestand oder Netzwerk zeigt immer den *von einem einzelnen Monitor gemeldeten wichtigsten Status* an, der zu ihm gehört. Im Folgenden werden Symbole gemäß Ihrer Wichtigkeit aufgelistet.

– Der Monitor ist deaktiviert.

– Dieses Symbol wird nur für Bestände und Netzwerke verwendet. Alle Monitore im Bestand oder Netzwerk sind deaktiviert, aber der Bestand oder das Netzwerk selbst sind aktiv.

– Der Monitor ist in einen Alarmstatus übergegangen.

– Der Monitor ist bei einem oder mehreren Tests fehlgeschlagen, ist jedoch noch nicht in den Alarmstatus übergegangen.

– Der Monitor ist in Ordnung.

Zusätzliche Richtlinien:

- Alle Status, mit Ausnahme des deaktivierten Status, sind aktivierte Status.
- Ein aktivierter Monitor prüft seinen Bestand.
- Durch Deaktivieren eines oder aller Monitore eines Bestands wird der Bestand nicht deaktiviert.
- Durch Deaktivieren eines oder aller Bestände eines Netzwerks wird dessen übergeordnetes Netzwerk nicht deaktiviert.
- Durch Deaktivieren eines Bestands werden seine *gesamten* Mitgliedsmonitore deaktiviert.
- Durch Deaktivieren eines Netzwerks werden seine *gesamten* Mitgliedsbestände deaktiviert.

Andere häufig verwendete Symbole

– Dieses Symbol zeigt die Eigenschaften eines Elements an und ermöglicht Ihnen, sie zu bearbeiten.

– Dieses Symbol zeigt an, dass ein Bestand oder ein Monitor von einer Vorlage übernommen wurde. Monitore, die von einer Vorlage übernommen wurden, können nicht direkt bearbeitet werden.

– Dieses Symbol zeigt an, dass sich ein Bestand oder ein Monitor im Wartungsstatus befindet und gegenwärtig nicht überwacht wird.

– Dieses Symbol zeigt eine Liste von Elementen an.

– Dieses Symbol zeigt eine Ansicht eines Elements an.

Hinweis: Siehe **Systemanforderungen** *(http://help.kaseya.com/WebHelp/EN/VSA/R8/reqs/index.asp#home.htm).*

Kapitel 1

Installation

In diesem Kapitel

Checkliste vor der Installation 4
Network Monitor Modulvoraussetzungen 4
Server Sizing 4
Installieren einer neuen Instanz von Network Monitor R8....5
Migration von KNM unabhängig zu KNM integriert 6
Übersicht zur Konfiguration 9

Checkliste vor der Installation

Es wird empfohlen die folgende Checkliste vor der Installation auszuführen, bevor **Network Monitor** installiert wird.

1. Schätzen Sie den erforderlichen Speicherplatz ein, der von **Network Monitor** benötigt wird, um die Anzahl an Beständen in Ihrem Netzwerk zu überwachen. Verwenden Sie dafür die Empfehlungen in **Server Sizing** *(siehe 4)*. Stellen Sie sicher, dass das System, das den **Network Monitor**-Server hostet, genügend Speicher hat, um **Network Monitor** auszuführen.
2. Überprüfen Sie, ob das System, das den **Network Monitor**-Server hostet, alle **Software- und Hardwareanforderungen** *(siehe 4)* erfüllt.
3. Wenn ein GSM-Telefon verwendet wird, müssen Sie dieses installieren und prüfen, ob es richtig auf Standard AT-Befehle in einem Terminalprogramm reagiert.

Wenn Sie diese Schritte ausgeführt haben, können Sie **Network Monitor** installieren.

Network Monitor Modulvoraussetzungen

Systeme, die Network Monitor R8 Server hosten

- Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2 mit dem neuesten Servicepaket
- Network Monitor hat eine eigene Datenbank und einen eigenen HTTP-Server
- Microsoft .NET Framework 4.5 oder höher

Unterstützte Browser

- Microsoft Internet Explorer 7.0 oder höher
- Opera 9.0 oder höher
- Chrome 8 oder höher
- Firefox 3.5 oder höher (Empfohlen für eine optimale Anzeige)

Die folgenden Merkmale müssen in den Browsereinstellungen aktiviert sein, um den Zugriff auf die Benutzeroberfläche zu ermöglichen.

- Cookies von Drittanbietern akzeptieren – Cookies sind erforderlich, um die Benutzersitzungen verfolgen zu können.
- Javascript aktiviert – Java-Skripte werden von der Webschnittstelle verwendet und müssen aktiviert sein.

Dienstprogramm Dashboard Map Editor

- Microsoft .Net Framework 4.0 oder höher

Server Sizing

Die empfohlenen Mindestanforderungen für **Network Monitor** hängen von der Anzahl an Beständen ab, die Sie überwachen wollen. Wir gehen von 10 Monitoren pro Bestand aus.

> **Hinweis:** Ein **Network Monitor Bestand** ist eine eindeutige IP-Adresse. Ein **Monitor** ist ein einziger Test oder eine Metrik dieses Bestands. Ein Windows-Rechner, der von einer einzigen IP-Adresse dargestellt wird, kann z. B. viele Monitore haben, wobei jeder Monitor Daten zu einer anderen Leistungsmetrik dieses Rechners zurückgibt.

Mindestanforderungen für bis zu 100 Bestände

- CPU mit 1 GHz
- 2 GB Speicher
- 5 GB freier Festplattenspeicher (1)

Mindestanforderungen für bis zu 250 Bestände

- CPU mit 2 GHz
- 2 GB Speicher
- 10 GB freier Festplattenspeicher (1)

Mindestanforderungen für bis zu 500 Bestände (3)

- 2-Kern-CPU mit >2 GHz
- 4 GB Speicher
- 15 GB freier Festplattenspeicher (1) (2)

Mindestanforderungen für bis zu 1000 Bestände (3)

- Intel 4-Kern-CPU mit 2 GHz
- 4 GB Speicher
- 25 GB freier Festplattenspeicher (1) (2)

Mindestanforderungen für bis zu 1500 Bestände (3)

- Intel 4-Kern-CPU mit 2 GHz
- 4 GB Speicher
- 40 GB freier Festplattenspeicher (1) (2)

Anmerkungen

[1] Angaben für eine jährliche Festplattennutzung bei normaler Installation mit der beschriebenen Anzahl an Beständen und Monitoren

[2] Kaseya empfiehlt, dass **Network Monitor** auf einem 1+0 RAID-Array mit mindestens 4 GB RAM installiert wird, um die bestmögliche Berichterstellungsleistung zu erzielen.

[3] Kaseya empfiehlt, dass Sie die Installation von **Network Monitor** auf einem dedizierten Rechner ausführen.

Installieren einer neuen Instanz von Network Monitor R8

Network Monitor R8 läuft nur als ein integriertes Add-On-Modul mit VSA.

So fügen Sie das Network Monitor R8 Add-On-Modul einer vorhandenen VSA R8 On-Premise-Umgebung hinzu:

1. **Senden Sie eine Supportanfrage** *(https://helpdesk.kaseya.com/home)*, um Ihre VSA-Lizenz aktualisieren zu lassen, sodass Sie Network Monitor R8 als ein Add-On-Modul installieren können.
2. Führen Sie **Kaseya Server Setup** *(http://help.kaseya.com/webhelp/DE/VSA/R8/install/index.asp#home.htm)* auf dem System aus, das Ihren Kaseya Server hostet. Klicken Sie auf Start > Alle Programme > Kaseya > **Kinstall**.
3. In Schritt **6. Geben Sie Ihren Kaseya-Lizenzcode** *(http://help.kaseya.com/webhelp/DE/KInstall/R8/index.asp#10338.htm)* des **Kaseya Server Setup** Installationsassistenten ein, akzeptieren Sie Ihren neuen Lizenzcode oder geben Sie ihn erneut ein und klicken Sie auf **Weiter**.
4. Stellen Sie die Installation oder Aktualisierung Ihrer VSA fertig.
5. Melden Sie sich bei Ihrer Instanz von VSA an und navigieren Sie zum Modul **Network Monitor**.

Migration von KNM unabhängig zu KNM integriert

Funktionsweise des Migrationsprozesses

Die VSA-gestützte Migration von Daten von **Network Monitor** unabhängig zu **Network Monitor** integriert ist ein Mapping-Prozess zwischen zwei Datasets.

Das Ziel des Mapping-Prozesses ist es, alle Bestände in der unabhängigen Konfiguration zu finden und mit einem entsprechenden Bestand in der VSA-Konfiguration zu verbinden. Auf diese Weise werden die Monitoring-Konfigurationen erhalten, die für jeden Bestand und dessen Schwellenwerte, Berichte, Aktionen, Zeitpläne und Verlaufsdaten angegeben werden.

Um diesen Mapping-Prozess erfolgreich durchzuführen, muss ein Netzwerk für jedes Gateway in der ursprünglichen unabhängigen Konfiguration sowie ein Gerät für jeden Bestand vorhanden sein, wobei das Gerät und die MAC-Adresse des Bestands übereinstimmen.

KNM-Konfiguration wird vorbereitet

- Stellen Sie sicher, dass Sie die aktuelle Version von KNM v5 (Build 9977) verwenden.
- Stellen Sie sicher, dass Ihre Lizenz die Anzahl der Geräte abdeckt, die zurzeit "unabhängig" sind.
- Entfernen Sie alle unnötigen Gateways und Geräte.
- Deinstallieren Sie alle Gateways auf deren Remote-Windows-Netzwerkrechnern.
  - Verwenden Sie die Programme hinzufügen/entfernen auf jedem Windows-Rechner, der ein Gateway hostet, um das Gateway zu deinstallieren. Falls nicht vorhanden, verwenden Sie `nmservice.exe -u` in einem Befehlsfeld, um das Gateway zu deinstallieren. Löschen Sie anschließend das `KNM`-Installationsverzeichnis, um alle übrigen Dateien zu löschen.
  - Navigieren Sie für das lokale Gateway zum Verzeichnis des lokalen Gateways und geben Sie `nmservicelg.exe -u` ein.
  - Verwenden Sie nach der Migration Agents, um Gateways zu installieren und deinstallieren.
- Archivieren Sie alle Protokolldateien im Verzeichnis `C:\kaseya\knm\logs` und löschen Sie anschließend diese Protokolldateien.
- Entfernen Sie alle Operatoren (KNM-Benutzer) von der unabhängigen Version, die über keinen Zugriff auf VSA verfügen.

Eingestellte Funktion und geänderte Merkmale

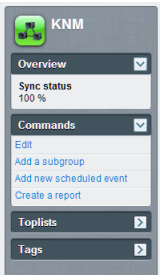
- Automatisches Anmelden ist eingestellt.
- **Network Monitor** verwendet das SSL-Zertifikat nicht mehr, dass durch den Parameter `WEBSERVER_CERT` in der Datei `init.cfg` angegeben wird. **Network Monitor**unterstützt noch die Verwendung eines SSL-Zertifikats, ist jedoch als Teil der VSA-Installation konfiguriert. Details siehe **Verwenden von SSL-Zertifikaten** *(http://help.kaseya.com/webhelp/DE/KInstall/R8/index.asp#18015.htm)*.
- Alle Konfigurationsdaten werden unter Verwendung von VSA auf den SQL-Server migriert.

Vor dem Installieren von VSA R8

1. Führen Sie die notwendigen Änderungen durch und bereinigen Sie die Konfiguration.
2. Kopieren Sie die gesamte KNM-Ordnerstruktur an einen sicheren Ort.
3. Führen Sie die Deinstallation für `Kaseya Network Monitor` unter Verwendung der Systemsteuerung durch.
4. Kopieren Sie den KNM-Ordner, der in Schritt 2 erstellt wurde, nach `%KASEYA_HOME%\knm`, wobei `KASEYA_HOME` der Ordner ist, in dem KInstall VSA installiert.
5. Zeigen Sie die Windows Services-Konsole an. Klicken Sie auf Aktion > Aktualisieren, um sicherzustellen, dass alle KNM-Services verschwunden sind, bevor Sie KInstall ausführen.

Nach dem Installieren von VSA R8

- Der Prozess `nmservice.exe` sollte jetzt ausgeführt werden. Die Datenbank `ksubscribers` sollte über einen neuen Namespace mit dem Namen `KNM` verfügen.
- Prüfen Sie die SQL-Server-Konvertierung in der resultierenden Protokolldatei `kaseya\knm\logs\fbmigrator_log.txt`.
- Beim ersten Start des integrierten Netzwerk-Monitor-Moduls in VSA wird das Modul im *Synchronisationsmodus ausgeführt.* VSA-Bestände, die im **Synchronisationsmodus** bestehen, werden mit den migrierten KNM-Gerätedaten verbunden. Die Schnittstelle zeigt nur die verbundenen Bestände und deren verbundene Entitäten an, z. B. Organisationen, Netzwerke und Maschinengruppen. **Der Fortschritt des Synchronisationsstatus** kann in der Eigenschaftenleiste auf der rechten Seite des Browsers angezeigt werden.



KNM wird automatisch neu gestartet, wenn 100 % Synchronisation erreicht wird. Wenn 100 % Synchronisation nicht erreicht werden kann, kann der Benutzer den Synchronisationsmodus manuell beenden, indem er den Konsolenbefehl `vsa-set-sync-complete` durchführt, der unten beschrieben wird, und den Service neu startet.

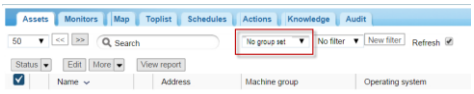
Häufige gestellte Fragen

Was passiert mit meinen Benutzern?

- Sie werden mit den Benutzern in VSA synchronisiert, wenn sie über denselben Namen verfügen. Führen Sie alle notwendigen Anpassungen in VSA oder KNM durch, bevor Sie die Konvertierung durchführen.

Ich erreiche keine 100 % Synchronisation Kann ich herausfinden, welche Bestände noch nicht synchronisiert sind?

- Ja, im Synchronisationsmodus ist eine zusätzliche Option "Kein Gruppenset" in der Auswahl Org/Gruppe verfügbar, die die Bestände anzeigt, die noch nicht synchronisiert sind.



Was tue ich, wenn ich einen nicht zugeordneten Bestand finde?

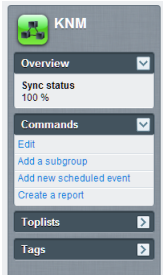
- Sie müssen sicherstellen, dass Discovery den Bestand im Netzwerk gefunden hat. Wenn der Bestand zu einem noch nicht ermittelten Netzwerk gehört, installieren Sie eine Agent-Sonde und scannen Sie das Netzwerk.

Muss ich 100 % Synchronisation erreichen?

- Nein, Sie wählen aus, was Sie migrieren und was Sie auslassen möchten. Wenn Sie mit dem zufrieden sind, was Sie in der Konfiguration sehen, können Sie die Synchronisierung jederzeit beenden, indem Sie die Systemadministrator-Befehlszeile verwenden.

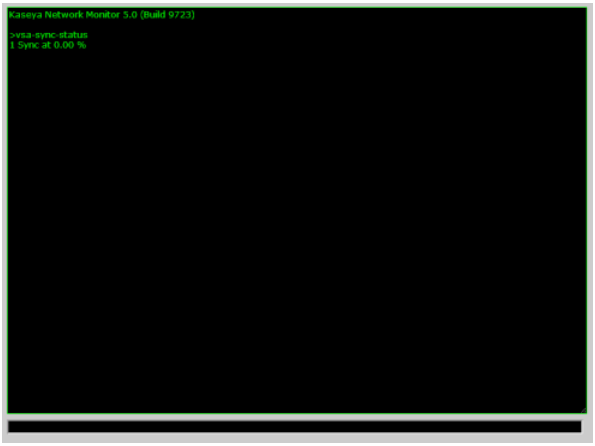
Wird der synchronisierte Anteil in Prozent irgendwo in der Schnittstelle angezeigt?

- Ja, in der Eigenschaftenliste des KNM-Knotens.



Welche Konsolenbefehle sind für diesen Vorgang verfügbar?

- `vsa-sync-status` - Zeigt den Status in Prozent pro Tenant an.
- `vsa-set-sync-complete` - Startet KNM nach einer erfolgreichen Synchronisierung neu.



Übersicht zur Konfiguration

Wenn **Network Monitor** R8 für Sie neu ist, ist die folgende Konfigurationssequenz geeignet, um das Produkt zu bewerten. Jeder Schritt enthält einen Link zu einer detaillierteren Erklärung, wie dieser Schritt ausgeführt werden soll.

1. Lesen Sie die Themen **Checkliste vor der Installation** *(siehe 4)*, **Server Sizing** *(siehe 4)* und **Network Monitor Modulvoraussetzungen** *(siehe 4)*.
2. Führen Sie die Schritte aus, die in **Installieren einer neuen Instanz von Network Monitor R8** *(siehe 5)* beschrieben sind.
3. **Melden Sie sich bei VSA** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#264.htm)* an.
4. Lesen Sie den Abschnitt **Erste Schritte** *(siehe 13)* dieser Dokumentation, um sich mit der Benutzeroberfläche des Moduls vertraut zu machen.
5. Führen Sie **Netzwerkermittlung** *(siehe 23)* aus.
6. **Installieren Sie ein Gateway** *(siehe 25)* in einem ermittelten Netzwerk.
7. **Fügen Sie den ausgewählten Beständen vorkonfigurierte Monitore** *(siehe 60)* hinzu.
8. Ändern Sie die Einstellungen für den Schwellenwert für den Monitor so, dass die Prüfung des Monitors fehlschlägt. Somit können Sie den **Fortschritt des Monitorstatus** *(siehe 53)* anzeigen.
9. Legen Sie **Aktionen** *(siehe 56)* fest, die ausgeführt werden, wenn ein Monitor eine bestimmte Anzahl nacheinander durchgeführter Prüfungen nicht besteht.
10. Prüfen Sie den Monitor, indem Sie einen Bericht für **Alarm simulieren** *(siehe 59)* erstellen, um sicherzustellen, dass der Alarm erwartungsgemäß konfiguriert ist.

Kapitel 2

Verwaltungsschnittstelle

In diesem Kapitel

Erste Schritte 13
VSA-Integration 22
Gateways 29
Untergruppen 42
Bestand 47
Monitore 53
Berichte 69

Erste Schritte

In diesem Abschnitt

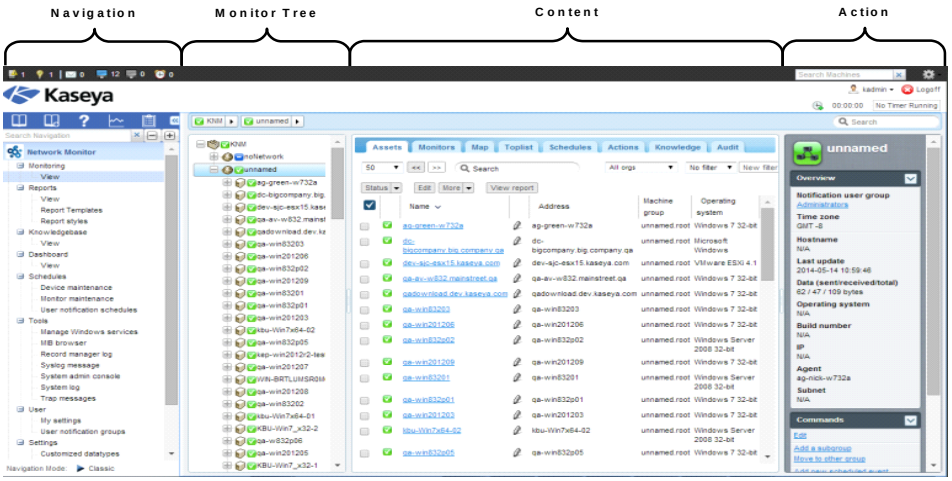
Die Monitoring-Ansicht 13
Monitorstruktur....14
Vererbung....15
Navigationsleiste 15
Listenansichten....15
Knoten- und Benutzersuche....16
Listenansichts-Steuerungselemente 17
Listenansicht filtern....17
Datenansichten....19
Eigenschaften und Befehle 20
Menüs bearbeiten....20
Verschieben von Knoten 21

Die Monitoring-Ansicht

Network Monitor > Monitoring > Ansicht

Die Network Monitor > Monitoring > **Ansicht** ist die Ansicht, mit der Sie in **Network Monitor** am meisten arbeiten. Bei Auswahl ist der Bildschirm in vier Fensterbereiche eingeteilt.

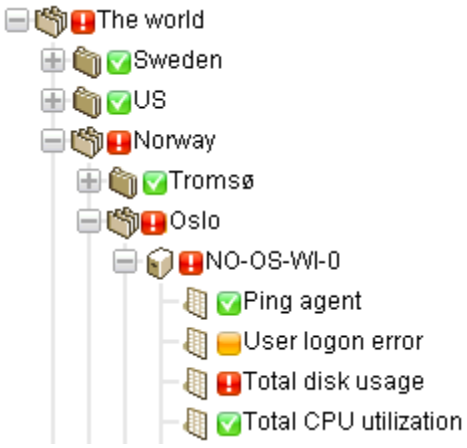
- **Navigation** – Zeigt die anderen drei Fensterbereiche an, wenn Sie das Element VSA > Network Monitor > Monitoring > **Ansicht** im Navigationsbereich auswählen. Andere Elemente im Navigationsbereich bieten Zugriff auf die **Einstellungen auf Modulebene und andere Ansichten** *(siehe 22)*.
- **Monitorstruktur** – Wählt Gruppe, Gateway, Bestand oder Monitor aus, mit dem gearbeitet werden soll.
- **Inhalt** – Zeigt Benutzerinhalt und Einstellungen an, wie z. B.. Bestände, Monitore oder Karten, entweder in einer Listenansicht, einer Datenansicht oder als Eigenschaftsblätter mit Registerkarten.
- **Aktion** – Zeigt die Haupteigenschaften und Befehle an, die Sie auf einem ausgewählten Knoten durchführen können.



Monitorstruktur

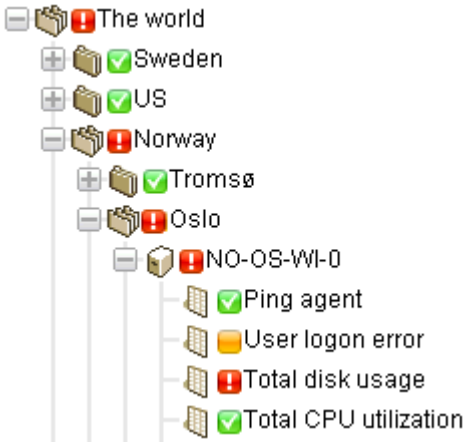
In der Monitorstruktur sind alle Gruppen, Gateways, Bestände und Monitore organisiert, die von **Network Monitor** verwaltet werden. Über die Struktur können Sie schnell zu einem beliebigen Bestand oder Monitor navigieren.

- **Gateways** – Ein Gateway überwacht Bestände, die dasselbe Subnetz nutzen. Bei einer Standardinstallation von **Network Monitor** gibt es nur ein `Local gateway` und es bezieht sich auf dasselbe Netzwerk, auf dem der **Network Monitor**-Server installiert ist.
- **Untergruppen** – Wird verwendet, um andere Knoten in der Monitorstruktur zu gruppieren. Untergruppen entsprechen keinem physischen Bestand in einem Netzwerk. Sie stehen vielmehr für logische Geschäftsbereiche, wie z. B. Unternehmen oder Abteilungen, oder ein Bestandsset innerhalb eines Netzwerks.
  - Ein Knoten kann nicht mehreren Elementen untergeordnet sein. Dazu gehört ein Untergruppenknoten.
  - Untergruppen können weitere Untergruppen haben.
  - Untergruppen können nur unter einem Gateway hinzugefügt werden.
- **Bestand** – Alles, was eine IP-Adresse hat. Dazu zählen Computer, Router, Switches, mobile Geräte, Drucker, Firewalls usw.
- **Monitore** – Ein Monitor führt einen bestimmten Test auf einem Bestand aus und meldet das Ergebnis dem Server. Ein Bestand kann mehrere Monitore haben.

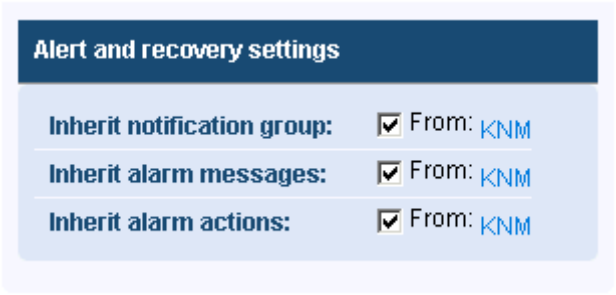


Vererbung

Bestimmte Knoteneigenschaften können von Knoten auf einer niedrigeren Stufe **geerbt** werden. Diese Designverbesserung betrifft fast alle anderen Aspekte der Konfiguration. Mit der Vererbung können Sie Konfigurationsänderungen auf hunderten, sogar tausenden Beständen und Monitoren mühelos verteilen, einfach durch Änderungen an einem Knoten auf einer höheren Stufe in der Monitorstruktur.

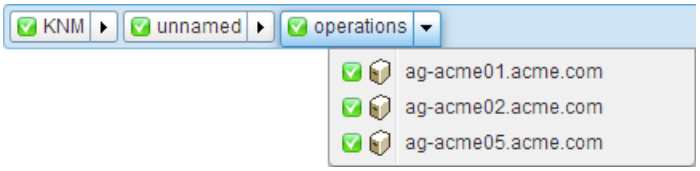


Bei jedem einzelnen Knoten können Sie wählen, ob Sie die geerbten Einstellungen verwenden oder sie überschreiben möchten. Die Darstellung unten zeigt z. B. eine Einstellung, die von einem übergeordneten Knoten geerbt wurde. Sie werden feststellen, dass diese Konvention in der gesamten **Network Monitor**-Benutzerschnittstelle bei vielen verschiedenen Eigenschaftstypen verwendet wird. *Beachten Sie, dass von einem Überschreiben einer geerbten Einstellung alle untergeordneten Knoten betroffen sind, die diese Änderungen erben.* Vererbung ist standardmäßig bei allen Beständen aktiviert, die sie unterstützen.



Navigationsleiste

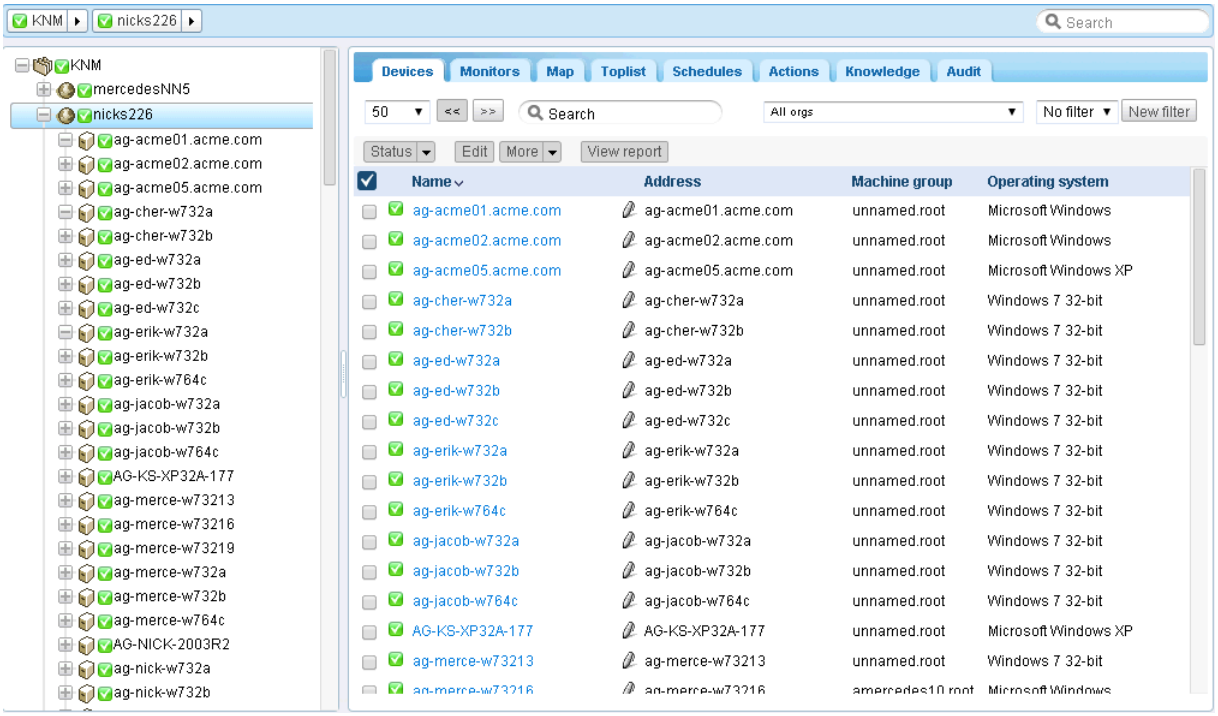
Der aktuell ausgewählte Knoten in der Struktur wird durch die Navigationsleiste oben in der Monitorstruktur angezeigt. Sie können auf eine beliebige Stelle in der Navigationsleiste klicken, um zu diesem Knoten in der Monitorstruktur zu gelangen. Sie können auch einen der untergeordneten Knoten des aktuell ausgewählten Knotens auswählen.



Listenansichten

Der mittlere Fensterbereich mit Registerkarten zeigt die Inhalte aller in der Monitorstruktur ausgewählten Knoten. Wenn der ausgewählte Knoten eine Gruppe, ein Gateway oder ein Bestand ist,

wird Ihnen eine Liste ähnlich der unten dargestellten angezeigt.



Ihnen werden Bestände und alle Monitore angezeigt, die Mitglieder dieser Gruppe oder dieses Gateways sind. Zum Beispiel:

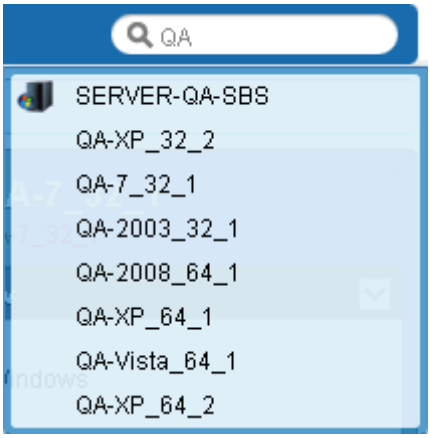
- Die Registerkarte **Bestand** zeigt alle *Bestände* an, die Mitglieder des ausgewählten Knotens in der Hierarchie sind.
- Die Registerkarte **Monitore** zeigt alle *Monitore* an, die Mitglieder des ausgewählten Knotens in der Hierarchie sind.

Knoten- und Benutzersuche

Das Bearbeitungsfeld **Suchen** wird in der oberen rechten Ecke angezeigt. Geben Sie eine Zeichenfolge ein, um die Monitorstruktur nach allen *Gruppen*-, *Gateway*- und *Bestands*knoten zu durchsuchen, die der eingegebenen Zeichenfolge entsprechen. **Drücken Sie nicht die Eingabetaste.** Warten Sie einfach, bis die Liste der Knoten unter dem Bearbeitungsfeld angezeigt wird und wählen Sie dann den anzuzeigenden Knoten aus.

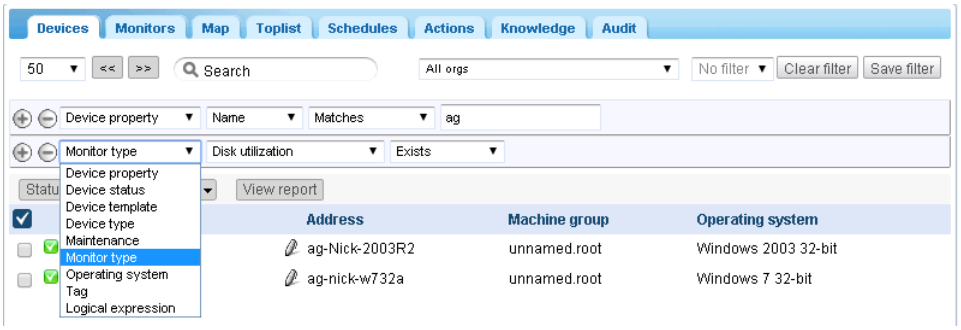
- Die Suche umfasst allen Text, der in das Feld **Beschreibung** eines Knotens eingegeben wurde.
- Die Suche umfasst die Namen und Beschreibungen von Benutzern und Benutzergruppen.

- Listenansichten zeigen in der Regel ein ähnliches **Such**feld, das Sie zum Filtern der Elemente in der Listenansicht verwenden können.



Listenansichts-Steuerungselemente

Bei jeder Listenansicht gibt es eine Reihe von Schaltflächen oben in der Liste, die auf mehrere Knoten in der Liste angewendet werden können. Sie können außerdem eine Seite vorwärts oder eine Seite rückwärts blättern sowie eine **Listenansicht filtern** *(siehe 17)*. Klicken Sie auf eine Spaltenüberschrift, um die Liste anhand dieser Spalte zu sortieren.



Listenansicht filtern

Filtern von Listenansichten durch Suche

Sie können die Listenansichten mithilfe des **Such**felds filtern. Die Daten, nach denen Sie suchen können, sind von der ausgewählten Listenansicht abhängig.

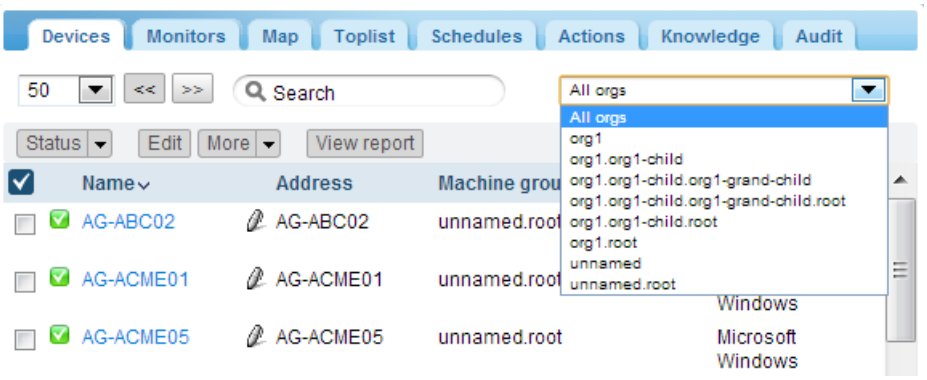
Bei Auswahl einer Gruppe	Registerkarte "Bestand"	Name, Beschreibung, Adresse und Rechnergruppenname
	Registerkarte "Monitore"	Name, Bestandsname, Rechnergruppenname
	Registerkarte "Zeitpläne"	Ereignis-/Zeitplanbeschreibung
	Registerkarte "Knowledge"	Artikel-ID, Artikeltitel
	Registerkarte "Audit"	Text der Mitteilung
Bei Auswahl eines Bestands	Registerkarte "Monitore"	Monitorname, Typ, (z. B. "CPU-Verwendung")
	Registerkarte "Knowledge"	Artikel-ID, Artikeltitel
	Registerkarte "Audit"	Text der Mitteilung
	Registerkarte	Text der Mitteilung

	"Statusänderung"	
Bei Auswahl einer Knowledge-Base-Kategorie	Artikel	Artikel-ID, Artikeltitel
	Audit	Text der Mitteilung

Filtern von Listenansichten nach Rechnergruppe und Unternehmen

Sie können jeden Knoten mit der Registerkarte **Bestand** oder **Monitore** im **Network Monitor**-Modul nach Unternehmen und Rechnergruppe filtern.

- Es wird eine zusätzliche Dropdownliste mit dem Standardwert `All orgs` angezeigt.
- Wählen Sie ein Element aus der `All orgs`-Dropdownliste aus, um die Bestands- bzw. Monitorliste nach diesem Wert zu filtern.



- Ihnen werden nur Unternehmen und Rechnergruppen angezeigt, für die Mitgliedsbestand im aktuellen Netzwerk gefunden wurde.
- Durch Klicken auf ein anderes Gateway in der Monitorstruktur wird normalerweise ein anderer Satz an Unternehmen und Rechnergruppen angezeigt.
- Welche Unternehmen und Rechnergruppen in der Liste für Sie sichtbar sind, ist abhängig von Ihrem ausgewählten VSA-**Scope** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#4578.htm)*.
- Durch das Filtern wird nicht die Anzeige des Bestands in der **Monitorstruktur** *(siehe 25)* beeinflusst.

Filtern von Listenansichten durch mehrere Bedingungen

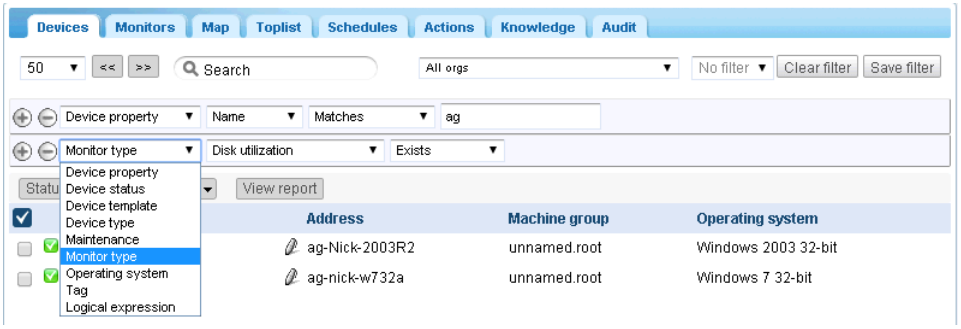
Die Listenansichten der Registerkarten Bestand und **Monitor** können nach *mehreren Kriterien* gefiltert werden. Zu den Filtertypen zählen:

- Bestandseigenschaft
- Bestandsstatus
- Bestandsvorlage – Der Bestand oder der Monitor ist mit einer Bestandsvorlage verknüpft oder nicht.
- Systemtyp
- Markierung
- Logischer Ausdruck

Die folgenden Aktionen sind mit bedingten Filtern verfügbar:

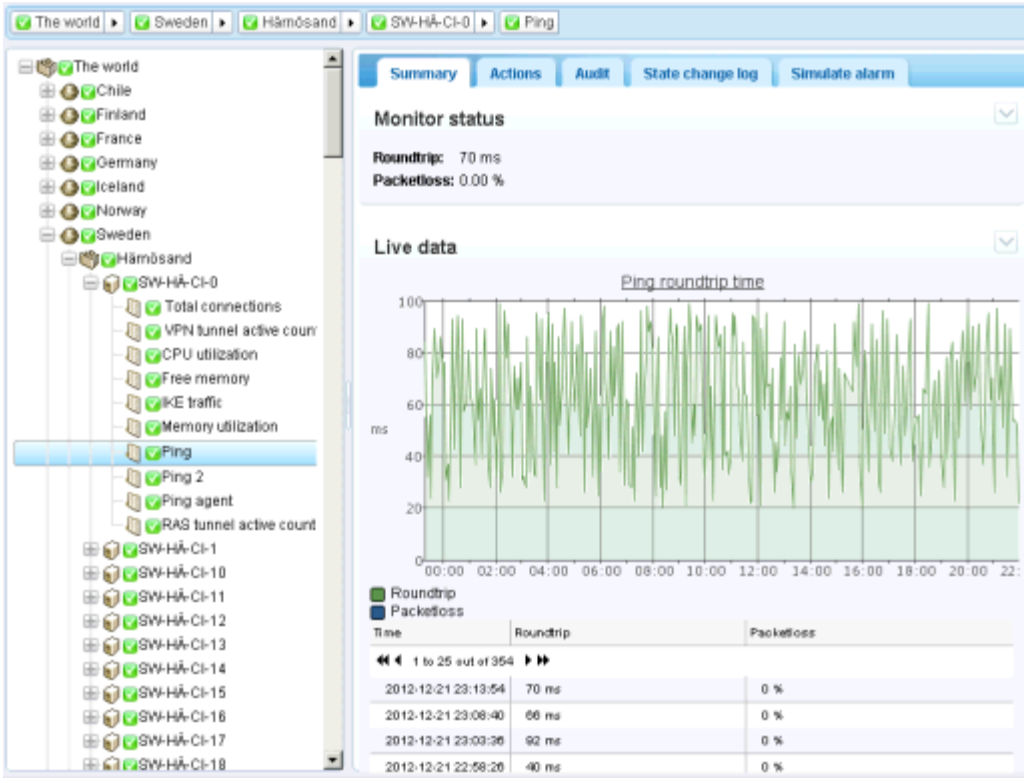
- **Neuer Filter** – Erzeugt einen neuen bedingten Filter.
- **Filter löschen** – Löscht einen bedingten Filter aus der Listenansicht.
- **Filter bearbeiten** – Zeigt einen gespeicherten bedingten Filter an, sodass Sie ihn bearbeiten können.
- **Filter speichern** – Speichert Änderungen an einem bedingten Filter.
- **Bearbeiten abbrechen** – Bricht die Bearbeitung von Änderungen an einem bedingten Filter ab.

- **Filter löschen** – Löscht einen bedingten Filter.



Datenansichten

Wenn es sich bei dem in der Monitorstruktur ausgewählten Knoten um einen Monitor handelt, zeigt die Registerkarte **Übersicht** die von diesem Monitor zurückgegebenen Daten an.



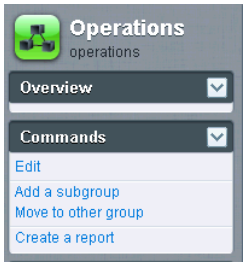
Eigenschaften und Befehle

Wenn eine Gruppe, ein Gateway, ein Bestand oder ein Monitor ausgewählt ist, werden im rechten Fensterbereich bestimmte Eigenschaften und Befehle angezeigt.

Untergruppenbefehle

Wenn eine **Untergruppe** ausgewählt wird, gibt es folgende gewöhnlich verwendete Befehle:

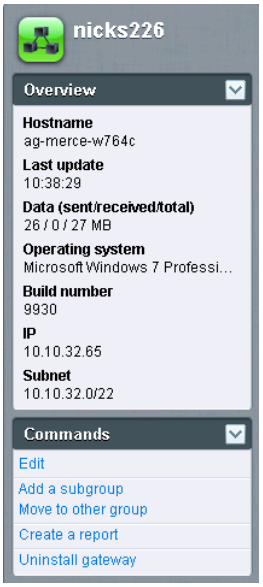
- Bearbeiten
- Untergruppe hinzufügen



Gatewaybefehle

Wenn ein **Gateway** ausgewählt wird, gibt es folgende gewöhnlich verwendete Befehle:

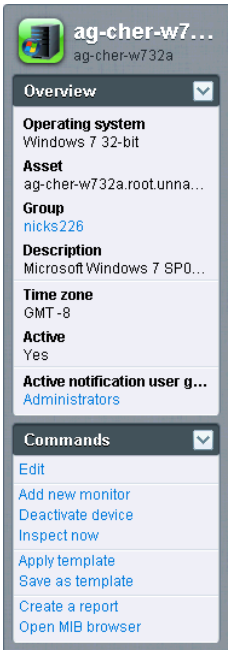
- Bearbeiten
- Untergruppe hinzufügen



Bestandsbefehle

Wenn ein **Bestand** ausgewählt wird, gibt es folgende gewöhnlich verwendete Befehle:

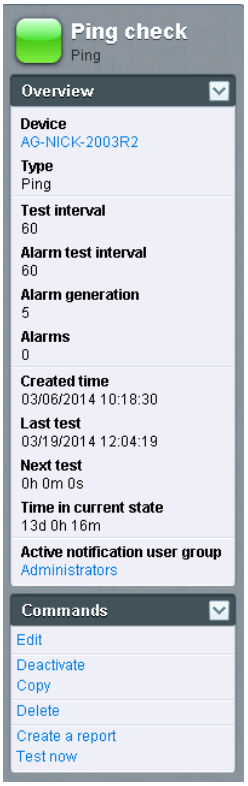
- Bearbeiten
- Neuen Monitor hinzufügen



Monitorbefehle

Wenn ein **Monitor** ausgewählt wird, gibt es folgende gewöhnlich verwendete Befehle:

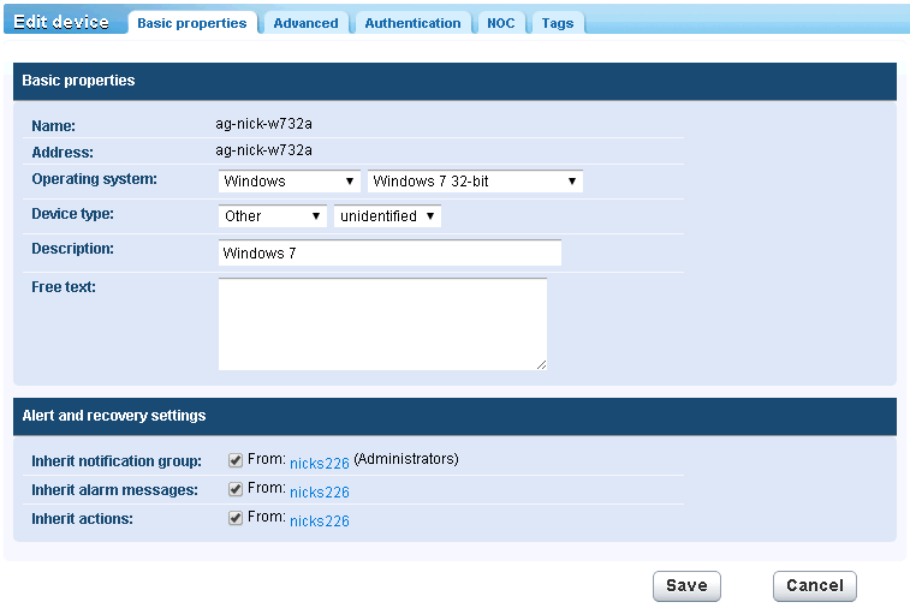
- Bearbeiten
- Jetzt testen



Menüs bearbeiten

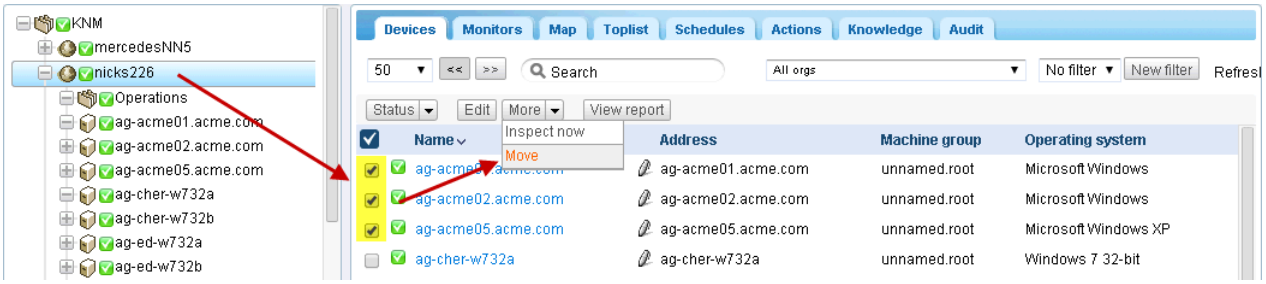
Wenn Sie auf den Befehl **Bearbeiten** bei einem ausgewählten Knoten klicken, sehen Sie in der Regel ein Blatt mit in Registerkarten dargestellten Eigenschaften. Bei den meisten Feldern wird beim Fahren mit dem Cursor darüber eine Quickinfo-Sprechblase rechts angezeigt, die eine Erklärung für das Feld bietet.

Klicken Sie auf die Schaltfläche **Speichern** oder **Abbrechen**, um das Bearbeitungsmenü zu schließen und zurück zur **Listenansicht** *(siehe 15)* oder zur **Datenansicht** *(siehe 19)* des ausgewählten Knotens zu kehren.

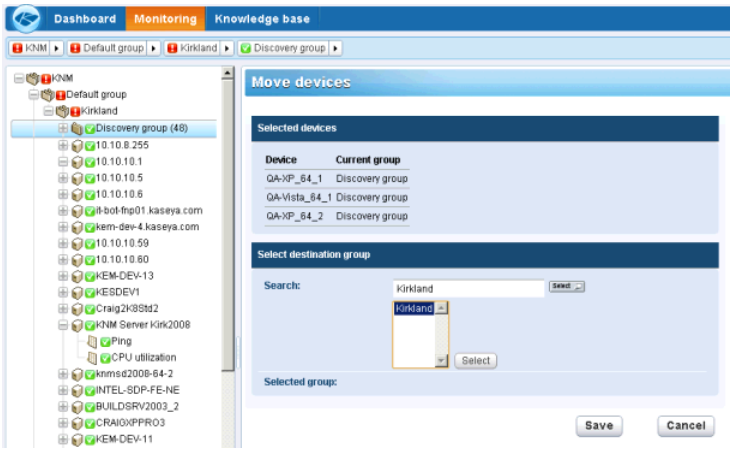


Verschieben von Knoten

Im Folgenden wird erklärt, wie die Monitorstruktur neu organisiert werden kann, indem ein Zweig der Monitorstruktur zur nächsten verschoben wird. Sie können Bestand nur zwischen Untergruppen *innerhalb desselben Gatewayknotens* verschieben.



1. Wählen Sie ein Gateway oder einen Gruppenknoten aus.
2. Wählen Sie den zu verschiebenden Bestand aus der Listenansicht aus.
3. Klicken Sie auf die Schaltfläche **Verschieben**. Die Seite **Bestand verschieben** wird angezeigt.



4. Geben Sie in das Bearbeitungsfeld **Suchen** Text ein, der dem Zielknoten entspricht. Es wird eine Dropdownliste möglicher Knoten angezeigt.
5. Klicken Sie auf den Zielknoten in der Dropdownliste.
6. Klicken Sie auf die Schaltfläche **Auswählen**. Der Zielknoten wird jetzt im Feld **Ausgewählte Gruppe** angezeigt.
7. Klicken Sie auf **Speichern**. Die Knoten werden jetzt an ihren neuen Speicherort in der Monitorstruktur verschoben.

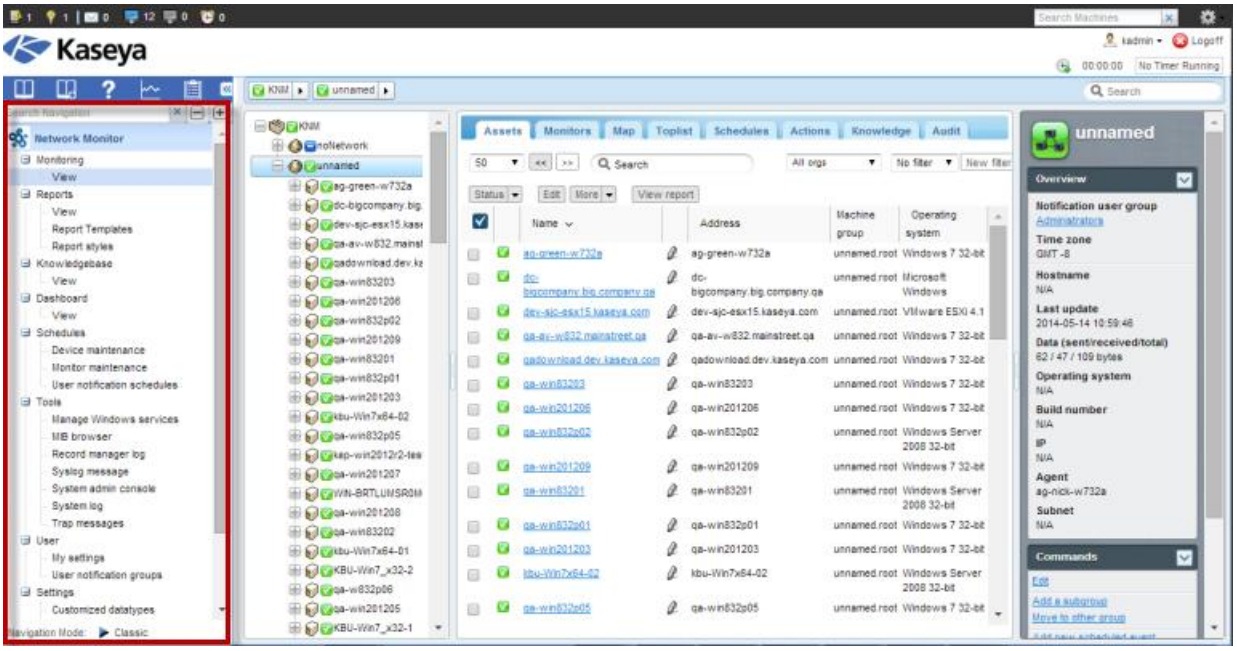
Hinweis: Sie können auch auf die Schaltfläche **Markieren** klicken, um nach einem Zielknoten zu suchen.

VSA-Integration

Überblick über das Navigationsfeld

Das Navigationsfeld von **Network Monitor** bietet unterschiedliche Inhaltsansichten und gibt Ihnen die Möglichkeit, Einstellungen auf Modulebene zu konfigurieren.

Hinweis: Das Navigationsfeld übernimmt die Funktion des ''K-Menüs'' in früheren, Standalone-Versionen von **Network Monitor**.



Diese Funktionen werden detailliert in den **Informationen zum Navigationsfeld** *(siehe 77)* ausgeführt, die in dieser Dokumentation enthalten sind. Bei Folgendem handelt es sich um eine beschreibende Zusammenfassung jeder Option des Navigationsfelds.

Funktionen	Beschreibung
Monitoring > **Ansicht** *(siehe 13)*	Wählt die **Monitoringansicht** *(siehe 13)* aus.
Berichte > **Ansicht** *(siehe 79)*	Konfiguriert benutzerdefinierte Berichte, die mit ausgewählten Knoten verbunden sind.
Berichtsvorlagen *(siehe 80)*	Konfiguriert Berichtsvorlagen, die mit allen Knoten verbunden werden können.

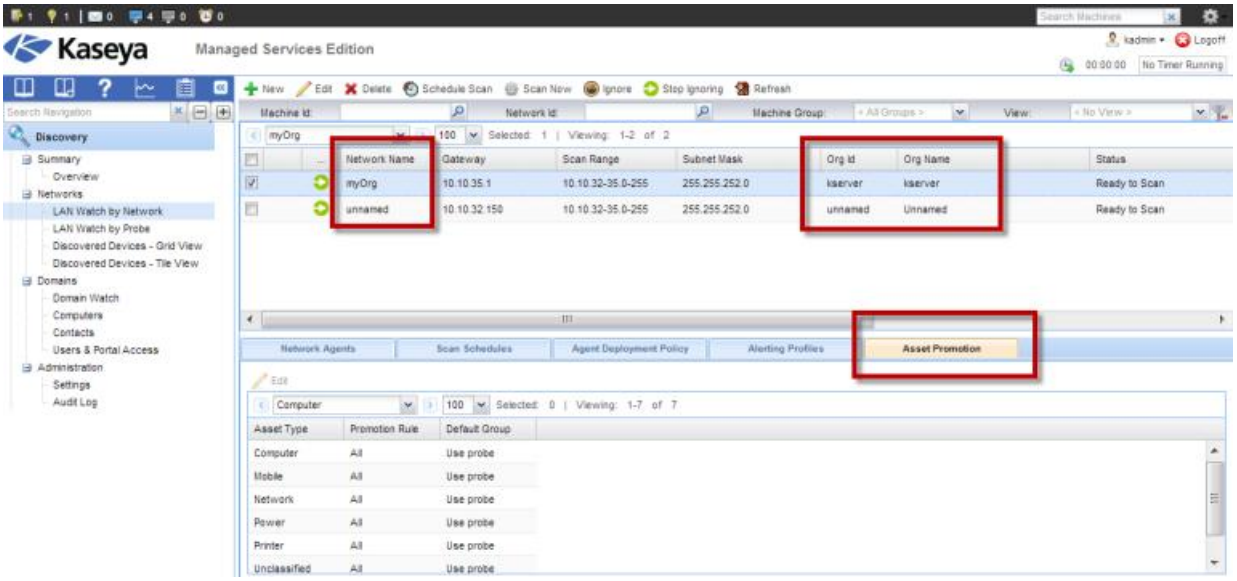
Berichtstile *(siehe 81)*	Konfiguriert das generelle Layout der Berichte, der Berichtsvorlagen und der benutzerdefinierten Berichte.
Knowledgebase > **Ansicht** *(siehe 89)*	Wählt die Ansicht "Knowledgebase" aus.
Dashboard > **Ansicht** *(siehe 92)*	Wählt die Ansicht "Dashboard" aus.
Bestandswartung *(siehe 93)*	Konfiguriert die Bestandswartungspläne.
Monitorwartung *(siehe 94)*	Konfiguriert Monitorwartungspläne.
Benutzerbenachrichtigungspläne *(siehe 95)*	Konfiguriert Network Monitor Benutzerarbeitspläne.
Management Windows Services *(siehe 96)*	Wählt die Ansicht "Management Windows Services" aus.
MIB-Browser *(siehe 97)*	Wählt die Ansicht "MIB-Browser" aus.
Datensatzmanagerprotokoll *(siehe 100)*	Wählt das Datensatzmanagerprotokoll aus.
Syslog-Meldung *(siehe 101)*	Wählt die Ansicht "Syslog-Meldungen" aus.
Systemadministratorkonsole *(siehe 102)*	Wählt die Ansicht "Systemadministratorkonsole" aus.
Systemprotokoll *(siehe 104)*	Zeigt vom `Kaseya Network Monitor` Service erstellte Protokolleinträge an.
Trap-Meldungen *(siehe 104)*	Wählt die Ansicht "SNMP-Trap-Meldung" aus.
Eigene Einstellungen *(siehe 104)*	Wählt die Ansicht "Eigene Einstellungen bearbeiten" aus.
Benutzerbenachrichtigungsgruppen *(siehe 105)*	Verwaltet Benutzergruppen. Bestandsbenachrichtigungen werden an alle Mitglieder der Benutzergruppe gesendet, die mit diesem Bestand verknüpft sind.
Angepasste Datentypen *(siehe 106)*	Erstellt benutzerdefinierte Datentypen zur Verwendung bei Monitoren, die generische Daten speichern können.
Bestandsvorlagen *(siehe 107)*	Konfiguriert Monitorsets, die einem Bestand in einem Schritt zugewiesen werden können.
Protokolleinstellungen *(siehe 108)*	Legt Protokollrichtlinien für Network Monitor fest.
NOC-Konfiguration *(siehe 109)*	Erstellt benutzerdefinierte NOC-Ansichten (Network Operations Center, Netzwerkbetriebsansichten).
Weitere Systemeinstellungen *(siehe 109)*	Legt weitere Einstellungen für Benachrichtigungen und andere Ereignisse fest.
SMS *(siehe 110)*	Legt SMS-Nachrichteneinstellungen fest.

Integration mit Discovery

Network Monitor verwendet das **Discovery**-Modul, um Netzwerkermittlungen auszuführen. Mit **Discovery** müssen Sie nur einen Agent auf einem einzigen Netzwerkrechner installieren, um alle anderen Geräte in diesem Netzwerk zu ermitteln. Sobald diese ermittelt wurden, wird das Netzwerk auf der Seite **LAN-Watch nach Netzwerk** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#10627.htm)* angezeigt, siehe unten.

- Wenn Sie zum ersten Mal mit Agents arbeiten, siehe Schnellstartanleitung **Agent-Bereitstellung** *(http://help.kaseya.com/webhelp/DE/VSA/R8/DE_agentdeployment_R8.pdf#view=Fit&navpanes=0)*.

- **Network Monitor unterstützt nicht das manuelle Hinzufügen oder Löschen von verwalteten Geräten (Beständen) innerhalb der Network Monitor-Module.** Ein Gerät muss von **Discovery** ermittelt und einem Bestand zugewiesen sein, um damit in **Network Monitor** arbeiten zu können.



Netzwerkermittlung

1. Navigieren Sie zur Seite Discovery Übersicht > **LAN-Watch nach Netzwerk** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#10627.htm)*.
2. Wählen Sie die Netzwerkzeile im oberen Feld aus und klicken Sie auf **Bearbeiten**.
3. Geben Sie einen **Netzwerknamen** ein, der leicht zu merken ist.
4. Legen Sie den IP-Suchbereich fest oder akzeptieren Sie den Standardwert.
5. Wählen Sie das Unternehmen aus, das mit diesem Netzwerk verknüpft ist.

> **Hinweis:** Mit der Zuordnung können Netzwerke in **Scopes** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#4578.htm)* eingeschlossen oder aus ihnen ausgeschlossen werden. Der Scope, den Sie mit Ihrer VSA-Benutzeranmeldung verwenden, bestimmt, ob Sie das Netzwerk in **Discovery** und den entsprechenden Gatewayknoten in **Network Monitor** sehen. *Die Zuordnung hat keinen Einfluss auf das Unternehmen und die Rechnergruppe, die den ermittelten Beständen zugewiesen sind.*

6. Speichern Sie, aber beginnen Sie noch nicht mit dem Suchen.

Bestandspromotion

Alle ermittelten Geräte, die Sie in VSA verwalten wollen, werden als "Bestände" bezeichnet und müssen mit einem Unternehmen und einer Rechnergruppe verknüpft werden, damit nach der Ermittlung mit ihnen gearbeitet werden kann. Agentbestände werden mit einem Unternehmen und einer Rechnergruppe verknüpft, wenn ein Agent installiert wird. Das Kennzeichnen eines Geräts als "Bestand", das kein Agent ist, wird als *Bestandspromotion* bezeichnet. **Network Monitor**überwacht nur *Bestände*.

Discovery automatisiert über die Registerkarte **Bestandspromotion** die höher Stufung eines Geräts auf einen Bestand. Standardmäßig werden alle ermittelten Geräte demselben Unternehmen und derselben Rechnergruppe zugewiesen wie der Test-Agent, mit dem Geräte im Netzwerk gesucht werden. Sie können nach Wunsch ermittelte Geräte verschiedenen Unternehmen und Rechnergruppen nach Bestandstypen zuweisen.

Scannen

Klicken Sie auf **Jetzt scannen**, um sofort mit der Ermittlung von Geräten im ausgewählten Netzwerk zu beginnen. Sie können mit der Schaltfläche **Suche planen** die Geräteermittlung auch regelmäßig einplanen.

Sobald die Suche beginnt, können Sie zum **Network Monitor**-Modul navigieren und sehen, wie Bestände in der **Monitorstruktur** *(siehe 25)* erscheinen.

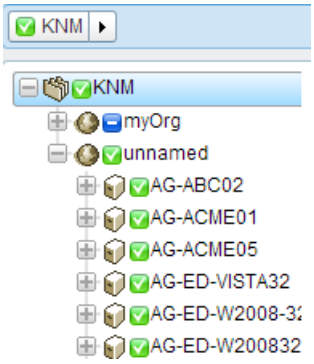
Gatewayknoten und Netzwerkermittlung

Gatewayknoten

Jedes von **Discovery** ermittelte Netzwerk wird als Gatewayknoten unter dem oberen `KNM`-Knoten in der Monitorstruktur angezeigt. Es gibt eine eindeutige Übereinstimmung zwischen Netzwerken, die in **Discovery** ermittelt wurden und Gatewayknoten, die in **Network Monitor** angezeigt werden. Sie können einen Gatewayknoten im **Network Monitor**-Modul von VSA nicht löschen.

Wenn Sie den Namen eines Netzwerks in **Discovery** ändern, wird der Name des Gatewayknotens im **Network Monitor**-Modul geändert.

Erweitern Sie jeden Gatewayknoten, um die im Netzwerk ermittelten Bestände und die als solche gekennzeichneten Bestände anzuzeigen. Die Liste der Bestände beinhaltet Computer und Geräte, die mit einem Agent installiert sind sowie Computer und Geräte, die keinen Agent haben, und **auf Bestand hochgestuft** *(siehe 23)* wurden.



Manuelles Hinzufügen von Untergruppen

Sie können Untergruppen Gatewayknoten hinzufügen. *Sie können Gruppen nicht über einen Gatewayknoten hinzufügen.* Bei regelmäßigen Suchen der Netzwerkermittlung werden erneut ermittelte Bestände nicht aus den Untergruppen verschoben, denen Sie zugewiesen sind.

Verschieben von Beständen

Sie können Bestände nur zwischen Untergruppen *innerhalb desselben Gatewayknotens* verschieben.

Installieren und Deinstallieren von Gateways

Gateways sammeln Monitoringdaten von Beständen, die mit demselben Netzwerk wie das Gateway verbunden sind. Das Gateway leitet dann Monitoringdaten an den **Network Monitor**-Server weiter.

Bei Gateways handelt es sich um Agent-Rechner, die Mitglieder eines **Netzwerks sind, das mit dem Discovery-Modul ermittelt wurde** *(siehe 23)*. Alle anderen Bestände des Netzwerks können ohne Agent bestehen bleiben und **Network Monitor** kann diese weiterhin überwachen. Der Agent-Rechner hostet die zusätzliche Gateway-Software, die sowohl zum Sammeln von Monitoringdaten sowie zu deren Übertragung auf den **Network Monitor**-Server erforderlich ist.

Installieren von Gateways

Wenn Sie noch kein Gateway für einen Gatewayknoten installiert haben, erscheint ein blaues Symbol . Dieses zeigt an, dass keine Verbindung zu den Beständen im Netzwerk möglich ist. So installieren Sie ein Gateway:

1. Wählen Sie den *Gatewayknoten* in der Monitorstruktur aus.
2. Klicken Sie auf den Befehl **Gateway installieren**.

3. **Wählen Sie Agent** in der Registerkarte **Einstellungen** aus. Wählen Sie einen Windows-basierten Agent-Rechner im ausgewählten Netzwerk aus und installieren Sie ein Gateway in diesem.
4. Klicken Sie auf die Registerkarte **Authentifizierung** und geben Sie Windowsanmeldedaten ein, damit Sie das Gateway installieren können.
5. Klicken Sie auf **Speichern**, um mit der Installation des Gateways zu beginnen.

In weniger als eine Minute werden alle blauen Symbole grün. Das heißt, dass eine Verbindung zu allen Beständen möglich ist und dass die Bestände Daten an den **Network Monitor**-Modulserver zurückgeben können. So können nun damit beginnen, Beständen **Monitore hinzuzufügen** *(siehe 59)* oder **vorkonfigurierte Monitore hinzuzufügen** *(siehe 60)*.

Deinstallieren von Gateways

Im selben Netzwerk können Sie ein Gateway auf einem Agent-Rechner deinstallieren und dieses Gateway auf einem anderen Agent-Rechner wieder installieren. Durch Deinstallation eines Gateways werden keine Bestände und Monitore deinstalliert, die Mitglieder dieses Gatewayknotens sind. Wird das Gateway auf einem anderen Agent-Rechner im selben Netzwerk neu installiert, so können Bestände und Monitore sich wieder verbinden und Daten ausgeben.

Unternehmen und Rechnergruppen

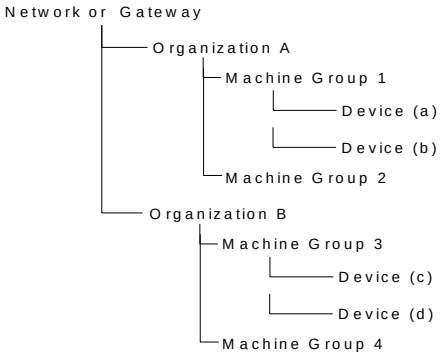
Unternehmen und Rechnergruppen sind logische "Container" in VSA, wo alle "Bestände" von VSA gewöhnlich verwaltet werden. Ein Bestand ist jeder Rechner oder Bestand, den Sie verwalten möchten. Innerhalb von VSA können Sie einen Bestand jeder Unternehmens- und Rechnergruppenkombination zuweisen.

Standardmäßige VSA-Hierarchien – Netzwerke, Unternehmen, Rechnergruppen und verwaltete Bestände – werden folgendermaßen im **Network Monitor**-Modul zugeordnet:

Discovery		Network Monitor
Netzwerke	→	Gateways
Organisationen/Rechnergruppen	→	Filtert Bestandslisten und Monitorlisten nach Unternehmen und Rechnergruppe.
		Erstellt Untergruppen unter einem Gatewayknoten.
Verwaltete Bestände (Rechner oder Bestand)	→	Bestand
		Monitore – hinzugefügt in Network Monitor

Netzwerkhierarchie

In jedem Netzwerk können verschiedene Unternehmen enthalten sein. Zum Beispiel können zwei unterschiedliche Teams einer Firma dasselbe Netzwerk für ein weitläufiges Projekt verwenden. In diesem Fall zeigt VSA ein einziges Netzwerk an, das Bestände von zwei verschiedenen Unternehmen und Rechnergruppen anzeigt.



Hinweis: Rechnergruppen und Unternehmen können verwendet werden, um in **Network Monitor** **Listenansichten zu filtern** *(siehe 17)*.

Umbenennen von Gateways und Beständen

Gateways oder ermittelte Bestände, die innerhalb des **Network Monitor**-Moduls **auf Bestand hochgestuft** *(siehe 23)* wurden, können nicht umbenannt werden. Wenn Sie diese Knoten bearbeiten, sehen Sie, dass die Namen schreibgeschützt angezeigt werden. Die Adressen der angezeigten Bestände in **Network Monitor** werden ebenfalls schreibgeschützt angezeigt. Navigieren Sie zum folgenden Standort, um die Namen der Gatewayknoten und Bestandsknoten zu ändern, die in **Network Monitor** angezeigt werden.

Netzwerke

- Benennen Sie das entsprechende Netzwerk eines Gateways über das Dialogfeld Discovery > **LAN-Watch nach Netzwerk** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#10627.htm)* > **Bearbeiten** um.
- Sie können mit dem Dialogfeld **Bearbeiten** darüber das Unternehmen ändern, das dem Netzwerk zugewiesen ist.

Ermittelte Bestände

So benennen Sie ermittelte Bestände *ohne Agent* um:

- Discovery > **Ermittelte Geräte – Rasteransicht** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#10619.htm)* > **Bestand umbenennen**
- Discovery > **Ermittelte Geräte – Titelansicht** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#10620.htm)* > **Bestand umbenennen**

Ändern Sie folgendermaßen das Unternehmen und die Rechnergruppen, die einem Bestand ohne Agent, der auf einen Bestand hochgestuft wurde, zugewiesen wurde:

- Audit > **Bestand anzeigen** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#10649.htm)* > **Gruppe ändern**

Ermittelte Geräte *ohne Agent* können aus der **Network Monitor**-Monitorstruktur entfernt werden. Verwenden Sie die folgenden "herabzustufenden" Geräte, die keinen Agent haben. Das heißt, dass Sie diese nicht länger in VSA verwalten möchten.

- Audit > **Bestand anzeigen** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#10649.htm)* > **Bestand auf Bestand herabstufen**

Ticket-Aktion

Die Aktion **Ticket** erstellt ein Ticket, wenn es durch eine Alarmzählung bei einem Bestand, der von **Network Monitor** überwacht wird, ausgelöst wird. Standardmäßig wird die Aktion **Ticket** von allen Beständen aus dem KNM-Gruppenknoten vererbt. Die Alarmzählung ist auf 1 eingestellt.

> **Hinweis:** Ein Ticket wird entweder im Modul **Ticketing** oder in **Service Desk** erstellt, abhängig davon, ob **Service Desk** innerhalb von VSA **aktiviert** *(http://help.kaseya.com/webhelp/DE/KSD/R8/index.asp#5478.htm)* wurde.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Benutzer** – Wählen Sie einen standardmäßigen VSA-Benutzer für die Aktion **Ticket** aus. Es handelt sich um den VSA-Benutzer, der dem erstellten Ticket zugewiesen wurde, wenn kein anderer VSA-Benutzer zugewiesen wurde.

Benutzerintegration

Benutzeranmeldungen für **Network Monitor** werden über System > **Benutzer** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#4576.htm)* erstellt.

- Der Zugriff auf Knoten innerhalb von **Network Monitor** wird über System > **Scopes** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#4578.htm)* verwaltet. Der Zugriff auf alle Knoten hängt von dem Unternehmen und der Rechnergruppe ab, mit der der Knoten verbunden ist und welcher ausgewählte Scope verwendet wird.
- Zugriff auf **Network Monitor**-Funktionen – wie z. B. Elemente im Navigationsfeld – werden über System > **Benutzerrollen** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#4577.htm)* verwaltet.
- Jeder VSA-Benutzer wird mit einer bestimmten E-Mail-Adresse definiert. Jeder Benutzer kann seine eigene E-Mail-Adresse über System > **Einstellungen** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#503.htm)* ändern.

> **Hinweis:** Siehe Schnellstartanleitung **Benutzer-Administration** *(http://help.kaseya.com/webhelp/DE/VSA/R8/DE_useradmin_R8.pdf#zoom=70&navpanes=0)* für weitere Informationen.

Benutzerbenachrichtigungsgruppen

Die **Benutzergruppenliste** *(siehe 105)* verwaltet Benutzergruppen, die von **Network Monitor** verwendet werden. Eine **Network Monitor**-Benutzergruppe enthält VSA-Benutzer.

Network Monitor Bestandsbenachrichtigungen werden an alle Mitglieder der Benutzergruppe gesendet, die mit diesem Bestand verknüpft sind. Dies erfolgt mithilfe der Einstellung **Benachrichtigung für Benutzergruppe** in der **Registerkarte "Basiseigenschaften"** *(siehe 50)* des Bestands.

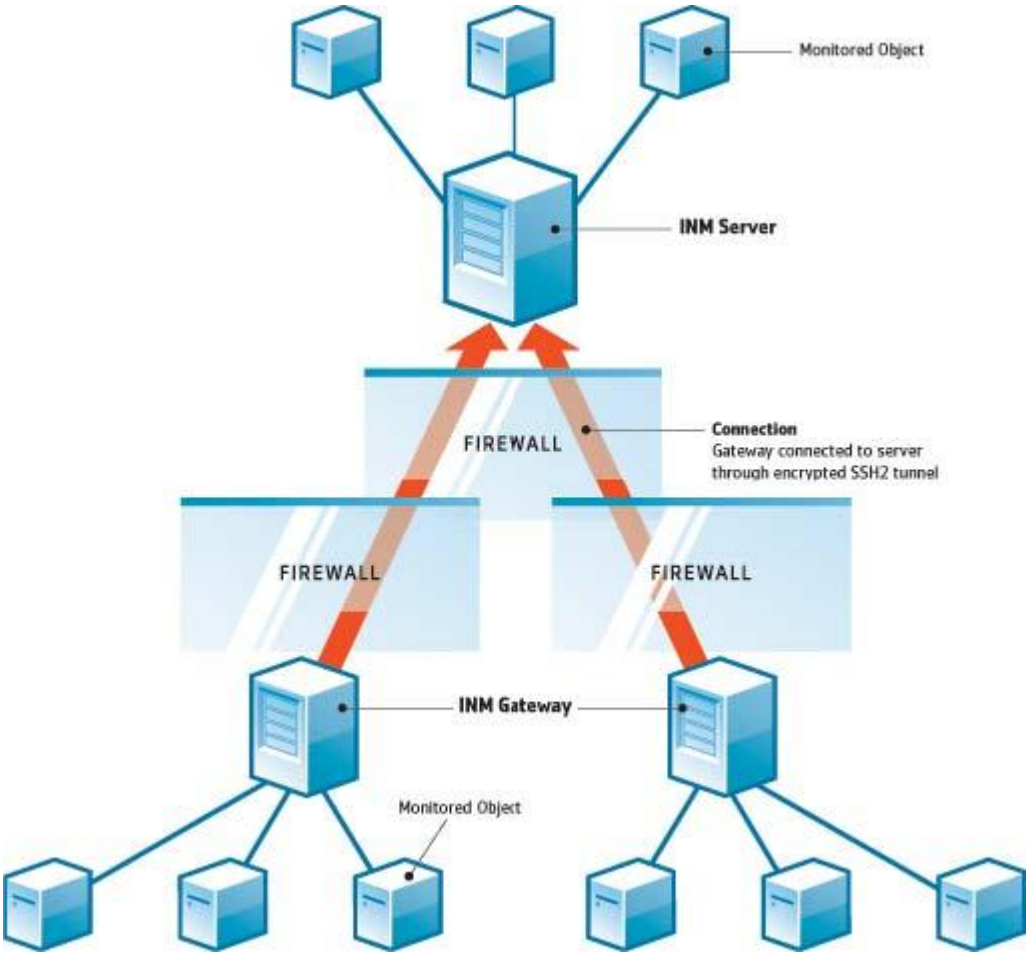
Network Monitor Lizensierung in VSA

Verwendete und verfügbare Lizenzen für **Network Monitor** werden auf der Seite VSA > System > **Lizenzmanager** *(http://help.kaseya.com/webhelp/DE/VSA/R8/index.asp#2924.htm)* angezeigt. Eine Agent-Lizenz wird für jeden Bestand ohne Agent (Rechner oder Gerät) verbraucht, der mit **Network Monitor** überwacht wird. Ein Rechner oder mobiles Gerät, auf dem bereits ein Agent installiert ist, verbraucht keine zusätzliche Agent-Lizenz, wenn es mit **Network Monitor** überwacht wird. Es wird eine

Agent-Lizenz für einen Bestand verbraucht, und zwar unabhängig von der Monitoranzahl für diesen Bestand.

Gateways

Network Monitor unterstützt das Monitoring von Servern, Routern und anderen Bestandstypen in *mehreren Netzwerken*. Ein **Gateway** wird im lokalen Netzwerk des Servers und auf allen von **Network Monitor** verwalteten Remote-Netzwerken installiert. Bestände werden vom Gateway überwacht, das sich im selben Netzwerk befindet. Jedes Gateway, ob lokal oder remote, sendet seine Überwachungsergebnisse zurück zum **Network Monitor**-Server.



Network Monitor Server

Der **Network Monitor**-Server enthält eine Datenbank und eine Verwaltungsschnittstelle, die einen konsolidierten Einblick in alle von allen Gateways zurückgegebenen Daten liefert. Remote-Gatewaybestände werden genauso verwaltet wie lokale Gateways. Dadurch ist **Network Monitor** sehr einfach zu konfigurieren und zu verwalten. Dieser Prozess ist für den Benutzer komplett transparent.

Network Monitor Gateway

Ein Gateway handelt auf Anforderungen vom Server hin. Gateways speichern bis auf eine kleine Cache-Datei lokal keine Konfigurations- oder Statistikdaten. Alle Daten werden sofort an den Server gesendet. Das Gateway muss auf einem Agent-Bestand installiert sein.

Server- und Gatewaykommunikation

Die Daten zwischen Gateway und Server werden immer vom Gateway zum Server gesendet. Der Grundgedanke ist, dass mehr Gateways als Server bereitgestellt werden, so dass der Administrator immer nur einen Port in der Firewall des Servers öffnen muss, um Kommunikation zuzulassen.

Wenn das Gateway sich aus irgendeinem Grund nicht mit dem Server verbinden kann, puffert das Gateway die Testergebnisse und Statistiken, während es auf den Server wartet. Diese Pufferungszeit kann bei jedem Gateway konfiguriert werden.

Sicherheit und Datenintegrität werden nach dem neuesten Stand der Technik mit dem Kommunikationsprotokoll SSH2 erzielt. Das SSH2-Protokoll verschlüsselt Daten mit Public-Key-Algorithmen und schützt Verbindungen vor Man-in-the-Middle-Angriffen. Genauso stellt auch VPN-Software sichere Tunnel im Internet her.

Zeitsynchronisierung

Network Monitor passt automatisch Zeitzonenunterschiede an. Die Administratoren müssen sicherstellen, dass die Uhren auf Gateways mit der Uhr im **Network Monitor**-Server synchronisiert sind. Wir empfehlen, Server und Gateways mit einem Zeitsynchronisierungsdienst wie z. B. NTP (Network Time Protocol) zu synchronisieren. Wird die Zeit zwischen Server und Gateway nicht synchronisiert, so **kann dies zu unvorhersehbaren Ergebnissen** bei Alarmerzeugung und Statistikspeicherung führen.

Gatewayknoten

Gatewayknoten werden als spezialisierte Knoten in der Monitorstruktur angezeigt. Gatewayanzeigen, -befehle und -eigenschaften gleichen denen von **Untergruppen** *(siehe 44)*. Gatewayknoten haben zusätzliche, spezielle **Eigenschaften und Befehle** *(siehe 30)* zur Verwaltung eines in einem Netzwerk installierten Gateways.

In diesem Abschnitt

Gatewaybefehle und -ansichten 30
Bearbeiten von Gateways 37

Gatewaybefehle und -ansichten

Befehle

Diese Befehle werden angezeigt, wenn ein Gatewayknoten ausgewählt wird, egal welche Ansichtsregisterkarte oben ausgewählt wurde.

- **Bearbeiten** - Bearbeitet die **Eigenschaften** *(siehe 44)* eines Gateways.
- **Untergruppe hinzufügen** – Erstellt eine **neue Untergruppe** *(siehe 44)* als untergeordneten Knoten.
- **In eine andere Gruppe verschieben** – Verschiebt das ausgewählte Gateway in eine andere Gruppe.
- **Eine Gruppe löschen** – Löscht den aktuell ausgewählten Gatewayknoten. Eine Gruppe, die über untergeordnete Knoten verfügt, kann nicht gelöscht werden.
- **Bestand hinzufügen** - Fügt manuell einen Bestand hinzu. Es müssen der Bestandsname, die IP-Adresse, der Agent, die Maschinengruppe und der Bestandstyp angegeben werden.
- **Ein neues geplantes Ereignis hinzufügen** - Fügt ein **geplantes Ereignis** *(siehe 35)* hinzu.
- **Bericht erstellen** – Erstellt einen **Bericht** *(siehe 69)*.
- **Gateway anwenden** - **Installiert ein Gateway** *(siehe 25)* auf einem Agent-Rechner.
- **Gateway deinstallieren** - Deinstalliert das Gateway, das zuvor vom Agent installiert wurde. Beim Deinstallieren eines Gateways werden keine Bestände und Monitore deinstalliert, die Mitglieder des Gatewayknotens sind. Durch das erneute Installieren des Gateways auf einem anderen Agent-Rechner können sich Bestände und Monitore erneut verbinden und Daten zurückgeben.

Ansichten

Gateways und Gruppen verwenden die gleichen Ansichten.

- **Registerkarte "Bestände"** *(siehe 31)* - Diese Registerkarte wird bei Gateways und Gruppen angezeigt.
- **Registerkarte "Monitore"** *(siehe 32)* - Diese Registerkarte wird bei Gruppen, Gateways und Beständen angezeigt.
- **Registerkarte "Karte"** *(siehe 32)* - Diese Registerkarte wird bei Gateways und Gruppen angezeigt.
- **Registerkarte "Toplist"** *(siehe 34)* - Diese Registerkarte wird bei Gateways, Gruppen und Beständen angezeigt.
- **Registerkarte "Zeitpläne"** *(siehe 35)* - Diese Registerkarte wird bei Gateways und Gruppen angezeigt.
- **Registerkarte "Aktionen"** *(siehe 56)* - Diese Registerkarte wird bei Gruppen, Gateways, Beständen und Monitoren angezeigt.
- **Registerkarte "Knowledge"** *(siehe 37)* – Diese Registerkarte wird bei Gateways, Gruppen und Beständen angezeigt.
- **Registerkarte "Audit"** *(siehe 37)* - Diese Registerkarte wird bei Gruppen, Assets und Monitoren angezeigt.

Registerkarte "Bestand"

Diese Registerkarte wird bei Gateways und Untergruppen angezeigt.

Die Registerkarte **Bestand** zeigt sämtlichen Bestand auf verschiedenen Stufen an, der Mitglied des ausgewählten Knotens in der Hierarchie ist.

Aktionen

Diese Aktionen sind oben in der Listenansicht verfügbar, wenn ein oder mehrere Bestände ausgewählt werden.

- **Status**
  - **Aktivieren** – Aktiviert ausgewählten Bestand und alle Monitore, die diesem Bestand zugewiesen sind.
  - **Deaktivieren** – Deaktiviert ausgewählten Bestand und alle Monitore, die diesem Bestand zugewiesen sind.
- **Bearbeiten** – Bearbeitet einen ausgewählten Bestand. *Wenn mehrere Bestände ausgewählt sind, werden nur Eigenschaften geändert, die in allen Beständen gleich sind.*
- **Mehr**
  - **Verschieben** – Verschiebt ausgewählten Bestand und alle Monitore, die diesem Bestand zugewiesen sind, in eine Untergruppe.
  - **Jetzt prüfen** – Prüft *mehrere* Bestände, um die geeigneten **vorkonfigurierten Monitore** *(siehe 60)* für diese Bestände zu bestimmen. **Jetzt prüfen** kann ausgeführt werden, wenn sich die Anmeldedaten oder die Konfiguration des Bestands geändert haben. Klicken Sie nach Ausführen von **Jetzt prüfen** bei jedem Bestand auf **Neuen Monitor hinzufügen**, um die Liste der vorkonfigurierten Monitore anzuzeigen.
- **Bericht anzeigen** – Erzeugt einen **Bericht** *(siehe 69)* für ausgewählten Bestand.

Tabellenspalten

- **Name** – Der Name des Bestands.
- **Adresse** – Der Netzwerkname oder die IP-Adresse.
- **Rechnergruppe** – Die dem in **Discovery** ermittelten Bestand zugewiesene Rechnergruppe.
- **Betriebssystem** – Der Systemtyp des Bestands.

Registerkarte "Monitore"

Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.

Die Registerkarte **Monitore** zeigt alle Monitore auf verschiedenen Stufen an, die Mitglieder dieses Knotens sind.

Aktionen

Diese Aktionen sind oben in der Listenansicht verfügbar, wenn ein oder mehrere Monitore ausgewählt werden.

- **Status**
  - **Alarm bestätigen** – **Bestätigt Alarme** *(siehe 68)* auf ausgewählten Monitoren.
  - **Aktivieren** – Aktiviert ausgewählte Monitore.
  - **Deaktivieren** – Deaktiviert ausgewählte Monitore.
- **Löschen** – Löscht ausgewählte Monitore.
- **Bearbeiten** – Bearbeitet einen ausgewählten Monitor. *Wenn mehrere Monitore ausgewählt sind, werden nur Eigenschaften geändert, die in allen Monitoren gleich sind.*
- **Jetzt testen** – Testet ausgewählte Monitore sofort.
- **Bericht anzeigen** – Erzeugt einen **Bericht** *(siehe 69)* für ausgewählte Bestände.

Tabellenspalten

- **Name** – Der Name des Monitors. Klicken Sie auf den Namen eines Monitors, um zu diesem Knoten zu gelangen.
- **Bestand** – Der Name des Bestands. Klicken Sie auf den Namen des Bestands, um zu diesem Knoten zu gelangen.
- **Typ** – Der **Typ des Monitors** *(siehe 115)*.
- **Status** – Der beim letzten Test ausgegebene Wert.

Registerkarte "Karte"

Diese Registerkarte wird bei Gruppen und Gateways angezeigt.

Die Registerkarte **Karte** zeigt eine große Karte an, wenn ein Knoten mit aktivierter Karte ausgewählt wird.

- Die große Karte skaliert sich automatisch, um die Standorte aller *untergeordneter Knoten* mit aktivierter Karte im ausgewählten Knoten zu umfassen.
- Durch Klicken auf das Standortsymbol auf der Karte gelangen Sie zu diesem Knoten in der Monitorstruktur. Wenn ein Symbol für mehrere untergeordnete Knoten *am selben Standort* steht, wird eine Liste der untergeordneten Knoten angezeigt. Durch Klicken auf einen untergeordneten Knoten gelangen Sie zu diesem Knoten in der Monitorstruktur.

Kleinere Karte

Eine kleinere Karte zeigt in der rechten unteren Ecke der Seite den Standort des *derzeit ausgewählten Knotens* an.

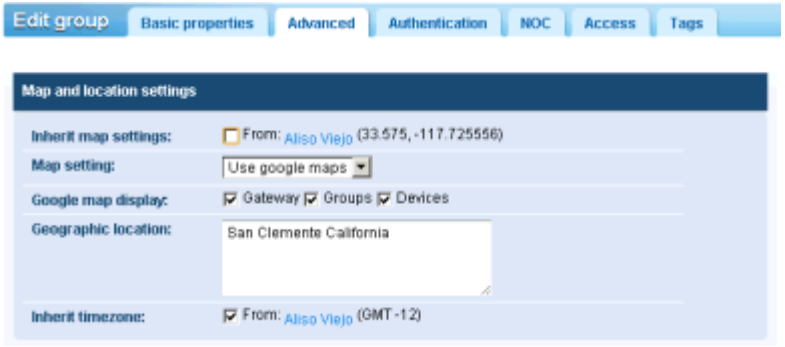
Vererbung

Gateways, Untergruppen und Bestand können mit einem Standort auf der Karte und einer lokalen Zeitzone verknüpft werden. Knoten auf einer niedrigeren Stufe können ihren geografischen Standort von den übergeordneten Knoten erben. Wird zum Beispiel der Standort eines Gateways oder einer Untergruppe für ein einzelnes Gebäude eingerichtet, so werden Standort und lokale Zeitzone für sämtliche Bestände im selben Gebäude wirksam eingestellt.

Konfiguration

Karteneinstellungen werden in der Regel in der Registerkarte **Erweitert** eines Knoten konfiguriert.

Network Monitorist in der API von Google Maps integriert. Das heißt, dass Sie entweder den *Namen eines Standorts* oder die *GPS-Koordinaten* in Dezimalschreibweise verwenden können, z. B. `-33.469048, -70.642007`, um den Standort eines Knotens zu identifizieren.



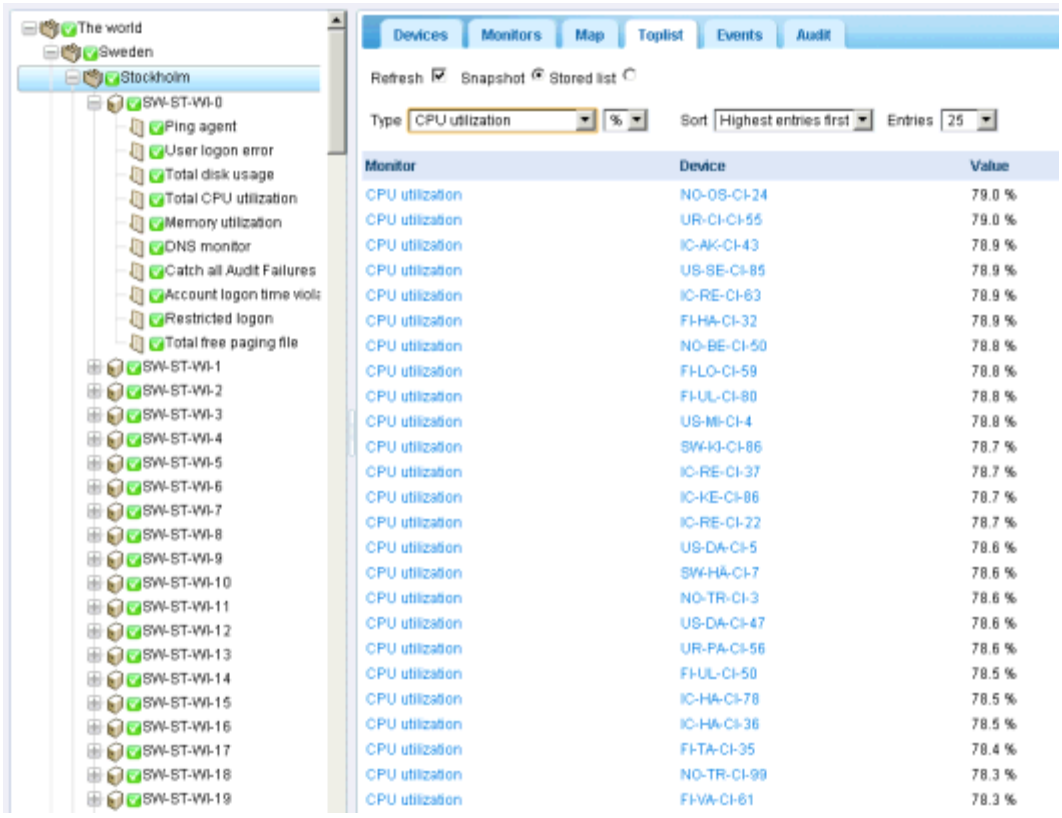
Karten- und Standorteinstellungen

- **Karteneinstellungen erben** – Bei Markierung werden **Karteneinstellungen** *(siehe 32)* vom übergeordneten Knoten geerbt und die anderen drei Kartenoptionen sind weiterhin ausgeblendet. Deaktivieren Sie dies, um Ihre eigenen Karteneinstellungen festzulegen.
  - **Karteneinstellung** – Karten von Google verwenden. Dies ist derzeit die einzige verfügbare Option.
  - **Anzeige auf Google-Karte** – Durch Aktivieren dieser Option legen Sie fest, ob Gateways, Gruppen und Bestände auf der Karte angezeigt werden.
  - **Geografischer Standort** – Geben Sie den *Namen eines Standorts* oder die *GPS Koordinaten* in Dezimalschreibweise ein, z. B. `-33.469048, -70.642007`.
- **Zeitzone** – Monitore zeigen ihre Echtzeitgrafiken in der Ortszeit des Bestands an.
  - **Zeitzone erben** – Bei Markierung werden Zeitzoneneinstellungen vom übergeordneten Knoten geerbt. Deaktivieren Sie dies, um Ihre eigene Zeitzone anzugeben.

Registerkarte "Toplist"

Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.

Die Registerkarte **Toplist** zeigt die Werte an, die von verschiedenen Beständen *für den gleichen Monitortyp* ausgegeben werden. Diese Werte werden fortlaufend in Echtzeit aktualisiert. Dadurch können Sie die Werte vergleichen und Monitore mit schlechter Leistung erkennen. Da für eine Toplist mehrere Bestände erforderlich sind, zeigen nur Gateways und Untergruppen die Registerkarte **Toplist** an. Auch **Berichte** *(siehe 88)* können Toplists umfassen.



Aktionen

- **Aktualisieren** – Bei Markierung wird die Seite aktualisiert.
- Wählen Sie eine der folgenden Optionen aus:
  - **Momentaufnahme** – Eine *Momentaufnahmen*-Toplist zeigt den letzten Wert für jeden Monitor in der Liste an.
  - **Gespeicherte Liste** – Die Toplists *Gespeicherte Liste* zeigen die *Min.*, *Max.* und *Durchschnitts*werte eines Monitors für ausgewählte tägliche, wöchentliche und monatliche Zeiträume an.
- **Laden** – Wird nur angezeigt, wenn **Gespeicherte Liste** ausgewählt ist. Zeigt die ausgewählte Toplist an.
- **Für Vergleich laden** – Vergleicht zwei Toplists.
  1. Wählen Sie eine *erste* und eine zweite Toplist aus und klicken Sie **Laden**.
  2. Wählen Sie eine *zweite* Toplist des gleichen **Typs** aus und klicken Sie dann auf **Für Vergleich laden**.

  Die *erste* Toplist wird links angezeigt. Die zweite Toplist wird rechts angezeigt. Nun sehen Sie, wie sich die überwachten Eigenschaften eines bestimmten Monitors zwischen den beiden Toplists verändert haben.

  Die folgende Option **Sortieren** kann nur bei einem Vergleich zweier Toplists verwendet werden.

  - `Top movers` – Einträge, die sich am meisten nach oben oder unten verschoben haben.
  - `Top climbers` – Einträge, die sich am meisten nach oben verschoben haben.
  - `Top fallers` – Einträge, die sich am meisten nach unten verschoben haben.
- **Typ** – Der Datentyp der Toplist und die Maßeinheit.
  - `CPU utilization`
  - `Disk utilization`
  - `Free disk space`
  - `Bandwith utilization`
  - `Ping roundtrip time`
  - `Ping packetloss`
  - `Free memory`
  - `Swap utilization`
  - `Webpage fetch time`
- **Daten**
  - `Sampled min value`
  - `Sampled max value`
  - `Period average`
- **Sortieren**
  - `Lowest entries first`
  - `Highest entries first`
- **Einträge** – Anzahl der angezeigten Einträge.

Tabellenspalten

- **Bestand** – Der Name des Bestands. Klicken Sie auf den Namen des Bestands, um zu diesem Knoten zu gelangen.
- **Monitor** – Der Name des Monitors. Klicken Sie auf den Namen des Monitors, um zu diesem Monitor zu gelangen.
- **Wert** – Der beim letzten Test ausgegebene Wert.

Registerkarte "Zeitpläne"

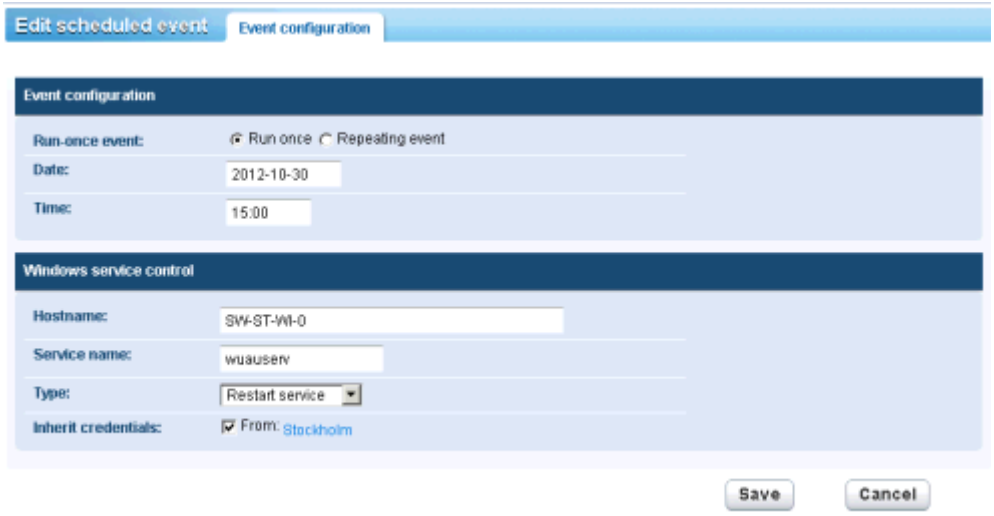
Diese Registerkarte wird bei Gateways und Untergruppen angezeigt.

Die Registerkarte **Zeitpläne** plant Aktionen für einen bestimmten Zeitraum (Datum und Zeit), statt auf einen Monitor zu warten, der diese Aktion auslöst. Ereignisse können geplant werden, um einmalig oder wiederholt ausgeführt zu werden.

> **Hinweis:** Ereignisse werden nicht vererbt. Jede Gruppe oder jedes Gateway kann ein beliebiges Ereignis für einen beliebigen Host planen. Aus Sicherheitsgründen *müssen Sie im Gatewayknoten oder in der Untergruppe geplante Ereignisse des Zielbestands verwenden.* Dadurch wird sichergestellt, dass geplante Ereignisse für diese Bestände nur durch Benutzer eingesehen werden können, die dafür autorisiert sind.

Klicken Sie auf die Registerkarte **Zeitpläne** eines beliebigen Gateways oder einer beliebigen Untergruppe. Die Registerkarte zeigt alle vorab geplanten Ereignisse an. Klicken Sie auf den Befehl **Geplantes Ereignis hinzufügen**. **Eine Liste der Ereignisaktionen wird angezeigt** *(siehe 163)*. Klicken Sie auf ein Ereignis, um dieses zu bearbeiten.

Die Konfigurationseinzelheiten hängen vom Typ der ausgewählten Ereignisaktion ab. Geben sie beim Festlegen eines Host den Hostnamen oder die IP-Adresse an. Wenn Sie ein Ereignis für einen Zielbestand von einer übergeordneten Gruppe oder einem Gateway aus planen, ist es wahrscheinlicher, dass Sie die angemessenen Anmeldedaten erhalten, falls diese erforderlich sind.



Planung

Alle Ereignisse bieten dieselben Planungsoptionen.

Ereignisse einmal ausführen

- **Datum** – Geben Sie das Datum ein.
- **Zeit** – Geben Sie die Zeit an.

Ereignisse wiederholen

- **Aktiv zwischen** – Gibt den Datumsbereich an, in dem sich das Ereignis wiederholt. Geben Sie den Datumsbereich im Format `YYYY-MM-DD` an. Werden diese Felder nicht ausgefüllt, wiederholt sich das Ereignis immer.
- **Wochentag** – Durch Markieren eines Tages wiederholt sich das Ereignis nur an den ausgewählten Tagen.
- **Tagesstunde(n)** – Die Stunde und Minute in der Sie jeden Tag das Ereignis wiederholen wollen. Das Format ist `HH:MM,HH:MM,...`
- **Letzter Tag im Monat** – Bei Markierung wiederholt sich das Ereignis am letzten Tag jedes Monats.
- **Tage im Monat** – Bei Markierung wiederholt sich das Ereignis an bestimmten Tagen im Monat. Geben Sie die Tage ein, getrennt durch ein Komma.

Registerkarte "Knowledge"

Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.

Die Registerkarte **Knowledge** zeigt die Liste der Knowledge-Base-Artikel an, die diesem Knoten zugewiesen sind.

Aktionen

- **Artikel hinzufügen** – Weist ausgewählte Artikel ausgewählten Gruppen und Beständen zu.
- **Artikel lösen** – Hebt die Zuweisung von ausgewählten Artikeln zu ausgewählten Gruppen und Beständen auf.

Verwandte Themen

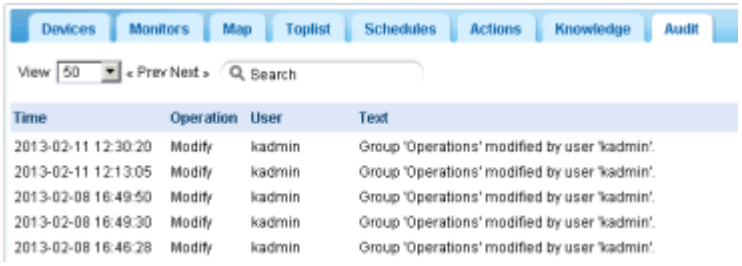
- **Knowledge-Base-Artikel** *(siehe 89)*
- **Knowledge-Base-Kategorien** *(siehe 91)*

Registerkarte "Audit"

Diese Registerkarte wird bei Gateways, Untergruppen, Beständen und Monitoren angezeigt.

Die Registerkarte **Audit** wird in jedem Knoten der Monitorstruktur angezeigt. Protokolleinträge beschreiben alle Konfigurationsaktionen, die von einem **Network Monitor**-Benutzer im aktuellen Knoten durchgeführt wurden.

> **Hinweis:** Bei Suchvorgängen muss auf Groß-/Kleinschreibung geachtet werden.


Devices
Monitors
Map
Toplist
Schedules
Actions
Knowledge
Audit
View 50 « Prev Next »
Search
Time Operation User Text
2013-02-11 12:30:20 Modify kadmin Group 'Operations' modified by user 'kadmin'.
2013-02-11 12:13:05 Modify kadmin Group 'Operations' modified by user 'kadmin'.
2013-02-08 16:49:50 Modify kadmin Group 'Operations' modified by user 'kadmin'.
2013-02-08 16:49:30 Modify kadmin Group 'Operations' modified by user 'kadmin'.
2013-02-08 16:46:28 Modify kadmin Group 'Operations' modified by user 'kadmin'.

Bearbeiten von Gateways

(ausgewähltes Gateway) > Bearbeiten

Die Seite **Gateway bearbeiten** konfiguriert die Eigenschaften eines Gatewayknotens. Gatewayknoten haben viele Eigenschaften mit **Untergruppen** *(siehe 44)* gemeinsam. Gatewayknoten haben zusätzliche, spezielle Eigenschaften und **Befehle** *(siehe 30)* zur Verwaltung eines in einem Netzwerk installierten Gateways.

- **Registerkarte "Basiseigenschaften"** *(siehe 38)* – Bei Gateways, Untergruppen und Bestand wird die Registerkarte **Basiseigenschaften** angezeigt.

- **Registerkarte "Erweitert"** *(siehe 38)* – Bei Gateways, Untergruppen, Bestand und Monitoren wird die Registerkarte **Erweitert** angezeigt.
- **Registerkarte "Authentifizierung"** *(siehe 40)* – Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.
- **Registerkarte "NOC"** *(siehe 41)* – Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.

Registerkarte "Basiseigenschaften" – Gateways

Bei Gateways, Untergruppen und Bestand wird die Registerkarte ''Basiseigenschaften'' angezeigt.

Basiseigenschaften

- **Name** – Geben Sie einen Namen für das Gateway ein.
- **Beschreibung** – Eine längere Beschreibung des Gateways.

Benachrichtigungs- und Wiederherstellungseinstellungen

- **Benachrichtigungsgruppe erben** – Legt die Benachrichtigungsgruppe für diesen Knoten fest. Sie können bei Gateways, Untergruppen und Bestandsknoten die Standardmeldung überschreiben, die an *Benutzergruppen* gesendet werden. Monitorknoten verwenden die Benachrichtigungsgruppe, die von ihrem übergeordneten Bestandsknoten bestimmt wird und nicht überschrieben werden kann.
- **Alarmmeldung erben** – Stellt das Format für **Alarmmeldungen** *(siehe 65)* dieses Knotens ein.
- **Aktionen erben** – Bei Markierung werden geerbte Aktionen und geerbte Wiederherstellungsaktionen in die **Registerkarte "Aktionen"** *(siehe 56)* dieses Knotens aufgenommen.

Registerkarte "Erweitert" – Gateways

Bei Gateways, Untergruppen, Bestand und Monitoren wird die Registerkarte ''Erweitert'' angezeigt.

Karten- und Standorteinstellungen

- **Karteneinstellungen erben** – Bei Markierung werden **Karteneinstellungen** *(siehe 32)* vom übergeordneten Knoten geerbt und die anderen drei Kartenoptionen sind weiterhin ausgeblendet. Deaktivieren Sie dies, um Ihre eigenen Karteneinstellungen festzulegen.
  - **Karteneinstellung** – Karten von Google verwenden. Dies ist derzeit die einzige verfügbare Option.
  - **Anzeige auf Google-Karte** – Durch Aktivieren dieser Option legen Sie fest, ob Gateways, Gruppen und Bestände auf der Karte angezeigt werden.
  - **Geografischer Standort** – Geben Sie den *Namen eines Standorts* oder die *GPS Koordinaten* in Dezimalschreibweise ein, z. B. `-33.469048, -70.642007`.
- **Zeitzone** – Monitore zeigen ihre Echtzeitgrafiken in der Ortszeit des Bestands an.
- **Zeitzone erben** – Bei Markierung werden Zeitzoneneinstellungen vom übergeordneten Knoten geerbt. Deaktivieren Sie dies, um Ihre eigene Zeitzone anzugeben.

Einstellungen von Gruppenabhängigkeit

- **Abhängigkeitsmonitor auswählen/Ausgewählte Monitore** – Geben Sie Text ein um die Namen der Monitore in der Liste **Abhängigkeitsmonitor auswählen** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie ein oder mehrere Monitore in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um die Monitore der Liste **Ausgewählte Gruppen** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielmonitoren zu suchen. Um einen Monitor zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.

Syslog-Meldungen empfangen

- **Syslog-Server** – Bei Markierung können Syslog-Meldungen, die im Gateway-Netzwerk abgefangen wurden, an den Server weitergeleitet werden. Nach der Markierung werden abgefangene Syslog-Meldungen auf der Seite Network Monitor > Werkzeuge > **Syslog-Meldung** *(siehe 101)* angezeigt.
- **Port** – Standardeinstellungen auf 514.

SNMP-Traps empfangen

- **SNMP-Trap** – Bei Markierung können SNMP-Trap-Meldungen, die vom Gateway-Netzwerk empfangen wurden, an den Server weitergeleitet werden. Für den **SNMP-Trap** *(siehe 142)*-Monitor muss dieses Kontrollkästchen markiert sein. Nach der Markierung werden empfangene Trap-Meldungen auf der Seite Network Monitor **>** Werkzeuge **Trap-Meldung** *(siehe 104)* angezeigt. Anhand der ausgewählten Meldungen können Sie SNMP-Trap-Monitore direkt auf den Seiten **Syslog-Meldung auflisten** erstellen.
- **IP** – Der Hostname oder die IP-Nummer des Trap-Empfängers.
- **Port** – Port-Nummer, den der Trap-Empfänger überwacht.
- **Community-Filter** – Die Community-Zeichenfolge des SNMP-Trap.
- **Filter für Agent-IP-Bereich** – Filtert das Weiterleiten von SNMP-Trap-Meldungen anhand der IP-Adresse.

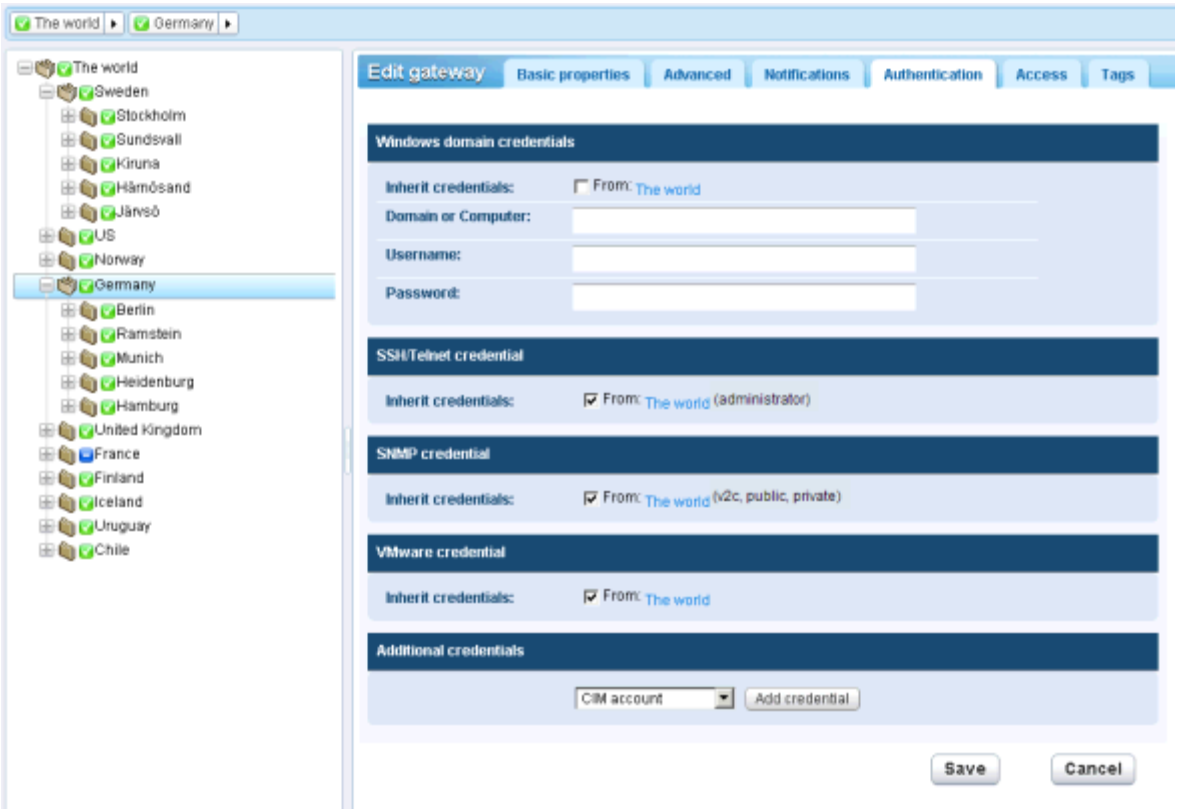
Sonstige Einstellungen

- **MIBs synchr.** – Bei Markierung wird dieses Gateway von **Network Monitor** automatisch mit MIB-Dateien aktualisiert, die dem Server hinzugefügt wurden.
- **Benachrichtigungsgruppe** – Gruppe, die per E-Mail benachrichtigt wird, wenn sich das Gateway nicht innerhalb eines bestimmten Zeitrahmens verbindet.
- **Automatisches Update deaktivieren** – Bei Markierung werden automatische Updates deaktiviert. Wenn diese Option nicht markiert ist, wird dieses Gateway automatisch mit der neuesten Version von **Network Monitor** aktualisiert, wenn der Server aktualisiert wird.

Registerkarte "Authentifizierung"

Diese Registerkarte wird bei Gateways, Untergruppen oder Bestand angezeigt.

Die Registerkarte **Authentifizierung** speichert die Anmeldedaten, die von **Network Monitor** zur Authentifizierung für den Zugriff auf Netzwerkbestand verwendet werden. Anmeldedaten werden *mithilfe von Vererbung* verwaltet. Das heißt, dass Sie die Anmeldedaten für ein einzelnes Gateway oder eine Untergruppe in der Monitorstruktur einstellen können und diese dann von allen untergeordneten Beständen und Monitoren verwendet werden. Außerdem können Sie sicher sein, dass diese Anmeldedaten niemals mit anderen Anmeldedaten verwechselt werden, die für andere Zweige in der Struktur eingestellt sind.



Wenn bei einem Authentifizierungstyp **Anmeldedaten vererben** markiert ist, werden die Anmeldedaten von einem Knoten auf höherer Stufe vererbt. Geben Sie die Anmeldedaten für diesen Authentifizierungstyp ein, wenn das Kontrollkästchen nicht markiert ist. Diese Anmeldedaten werden von diesem Knoten und allen Knoten auf niedrigerer Stufe verwendet, die diesen Authentifizierungstyp erben. *Wenn der Name der angegebenen Anmeldedaten nicht neben dem Namen des übergeordneten Knotens in Klammern angezeigt wird, bedeutet das, dass die Anmeldedaten bisher noch nicht auf einem übergeordneten Knoten definiert wurden.*

Die Authentifizierungstypen umfassen:

- **Anmeldedaten von Windows-Domäne** – Gibt lokale oder Domänen-Anmeldedaten von Windows an. Lassen Sie das Feld **Domäne oder Computer** leer oder geben Sie `localhost` ein, um die Anmeldedaten von localhost anzugeben. Gilt für mehrere **Monitore, die Windows-Authentifizierung verwenden** *(siehe 190)*.
- **SSH-Telnet-Anmeldedaten** – Gibt SSH- und Telnet-Anmeldedaten an.
- **SNMP-Anmeldedaten** – Gibt SNMP-Anmeldedaten an. Die erforderlichen Parameter hängen von der SNMP-Version ab, die zur Verbindung mit dem Bestand verwendet werden:
  - **SNMP v1** oder **SNMP2c** – Geben Sie den Namen der **Community mit Lesezugriff** und den Namen der **Community mit Schreibzugriff** ein.

- **SNMP v3** – Wenn Authentifizierung erforderlich ist
  - ✓ **SNMPv3 Context ID** – Optional. Eine Zeichenfolge, die einer oder mehreren Context-IDs entspricht, welche vom SNMP-Agent im Bestand angegeben wurden, um die ausgegebenen Daten zu begrenzen.
  - ✓ **Authentifizierungsmethode** – Der zur Authentifizierung verwendete Algorithmus: `None`, `HCMA-MD5` oder `HCMA-SHA1`.
  - ✓ **SNMPv3-Benutzername** – Der Name des SNMP-Managers, der für den Zugriff auf den SNMP-Agent im Remote-Bestand verwendet wird.
  - ✓ **SNMPv3-Passphrase** – Eine Abfolge von Wörtern, einem Kennwort ähnlich.
  - ✓ **SNMPv3-Verschlüsselung** – Der Algorithmus, der verwendet wird, um den Datenschutz mithilfe von Datenverschlüsselung sicherzustellen: `None`, `DES` oder `AES-128`.
  - ✓ **SNMPv3-Kryptografieschlüssel** – Die Zeichenfolge, die zur Datenverschlüsselung verwendet wurde.

- **VMWare-Anmeldedaten** – Gibt die VMWare-Anmeldedaten an.
- **Zusätzliche Anmeldedaten** – Sie können für Folgendes zusätzliche Anmeldedaten hinzufügen.

```
CIM account
Exchange account
FTP account
HTTP account
IMAP account
LDAP account
MySQL account
ODBC account
Oracle account
POP3 account
RADIUS account
SMTP account
SQL server account
```

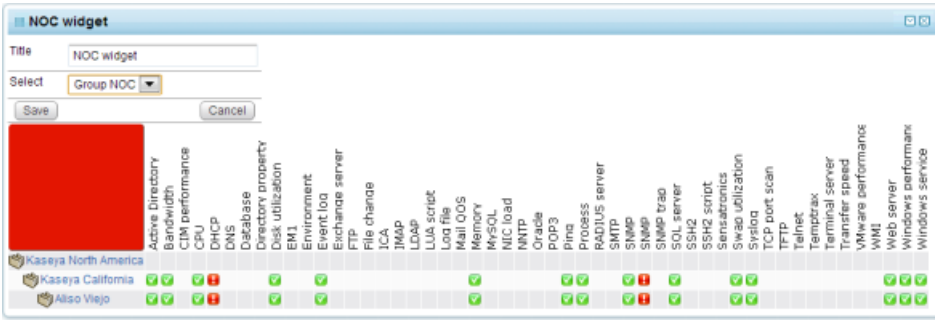
Registerkarte "NOC"

In dieser Registerkarte werden entweder Gruppen, Gateways oder Bestände angezeigt.

In der Registerkarte **NOC** (Network Operation Center, dt. Netzwerkbetriebszentrum) können Sie einen Gruppen-, Gateway- oder Bestandsknoten einer *NOC-Ansicht* zuordnen.

NOC-Widgets sind kompakte Vollbildansichten mit Informationen zum Status einer Ansammlung von Netzwerken und Beständen. Sie werden normalerweise auf dedizierten Monitoren angezeigt.

In NOC-Ansichten werden Gruppen-, Gateway- und Bestandsstatus hierarchisch geordnet und in einem Matrixformat angezeigt. Alle Gruppen, Gateways und Bestände werden in vertikaler Ausrichtung aufgelistet, während der Status für jeden Monitortyp horizontal aufgeführt wird. Der Gesamtstatus geht aus dem großen farbigen Rechteck auf der linken Seite hervor.



Konfigurieren einer NOC-Ansicht und eines NOC-Widgets

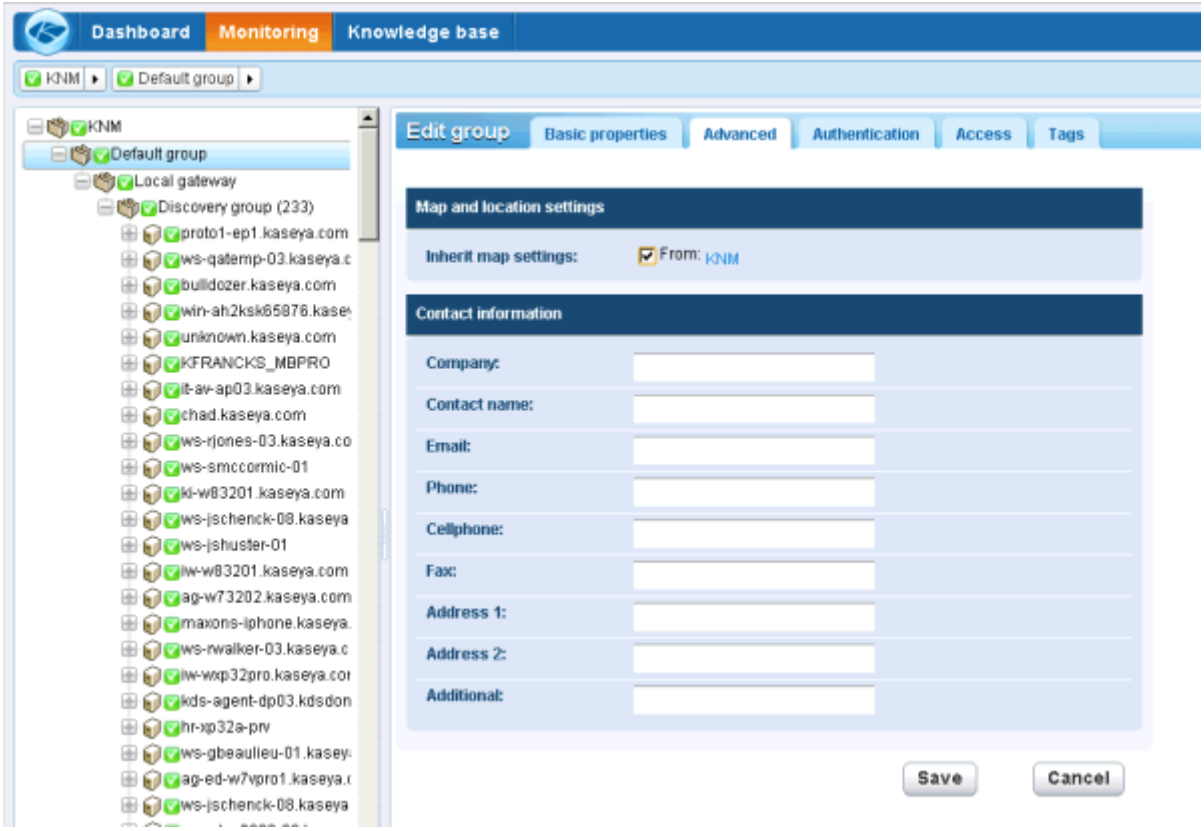
1. Auf der Seite Network Monitor-Einstellungen > **NOC-Konfiguration** *(siehe 109)* können Sie eine oder mehrere NOC-Ansichten konfigurieren.
2. Es muss mindestens einer NOC-Ansicht ein **Gatewayknoten** oder ein **Untergruppenknoten** über die Registerkarte Bearbeiten > **NOC** zugeordnet werden.
3. Wählen Sie "Dashboard > Widget hinzufügen > **NOC-Widget**" aus.
4. Wählen Sie das Symbol ☑ auf der rechten Seite der Titelleiste des Widgets aus, um die folgenden Einstellungen zu konfigurieren:
   - **Titel** – Der Titel des NOC-Widgets, der im Dashboard angezeigt wird.
   - **Auswählen** – Wählen Sie die Standardansicht `Group NOC` oder eine andere NOC-Ansicht, die Sie erstellt haben.

Untergruppen

Untergruppen sind "Container"-Knoten, die zur Gruppierung anderer Knoten *unterhalb eines Gateways* in der Monitorstruktur verwendet werden.

- **Logische Geschäftsbereiche** – Eine Untergruppe kann einen logischen Geschäftsbereich darstellen. Ändern Sie den Namen der Untergruppe, um den Namen des Geschäftsbereichs wiederzugeben. Wenn Sie eine Untergruppe **bearbeiten**, klicken Sie auf die Registerkarte **Erweitert**. Sie werden bemerken, dass Kontaktinformationen für den Geschäftsbereich eingegeben werden können, den eine Untergruppe darstellt. Wenn bei einem Bestand ein Eingriff vor Ort erforderlich ist, zeigen Sie den nächst höheren Bestand im der Monitorstruktur an, um die erforderlichen Kontaktinformationen zu erhalten.

- **Spezialisierte Dienstanforderungen** – Auch wenn ein Bestand keinen anderen Geschäftsbereich darstellt, müssen Sie eventuell spezialisierte Dienste für eine Bestandsgruppe innerhalb eines Subnetzes erbringen. Am einfachsten ist es, diese Bestände durch Gruppierung beieinander zu unterscheiden. In diesem Fall können Sie die Untergruppe in den Abteilungsnamen umbenennen oder in den Dienst, den Sie leisten.



Vererbung durch Untergruppe

Untergruppen können viel mehr als nur Organisieren und Kennzeichnen. Wenn Sie eine Untergruppe bearbeiten, merken Sie, dass sie viele Eigenschaften enthält, z. B. Benachrichtigungseinstellungen, Authentifizierung, Zugriff und Kartenstandorte. Damit können Sie die Eigenschaften aller untergeordneten Bestände der Untergruppe mithilfe von Vererbung einstellen. Dies kann verschachtelte Untergruppen, Bestand und Monitore umfassen.

Wenn Sie sich die Zeit nehmen, die von Ihnen verwalteten Bestände nach Untergruppe zu organisieren und die Vererbungsfunktion zu verwenden, kann erheblich Zeit beim einzelnen Konfigurieren von Bestand sparen.

Der Stammknoten

Der Knoten auf oberster Stufe, standardmäßig als `KNM` bezeichnet, ist tatsächlich der übergeordnete Gruppenknoten. Die für den Stammknoten eingestellten Gruppeneigenschaften können von Knoten auf niedrigeren Stufen *geerbt* werden, genauso wie alle Untergruppen, die Sie erstellen. Im Stammknoten können Einstellungen potenziell *von allen anderen Knoten in der Monitorstruktur geerbt werden.*

In diesem Abschnitt

Gruppenbefehle und Ansichten 44
Hinzufügen / Bearbeiten von Untergruppen 44

Gruppenbefehle und Ansichten

Befehle

Die gleichen Befehle werden angezeigt, wenn ein Gruppenknoten ausgewählt wird, unabhängig von der oben ausgewählten Ansichtsregisterkarte.

- **Bearbeiten** – Bearbeitet die **Eigenschaften** *(siehe 44)* einer Gruppe.
- **Untergruppe hinzufügen** – Erstellt eine **neue Untergruppe** *(siehe 44)* als untergeordneten Knoten.
- **In eine andere Gruppe verschieben** – Verschiebt die aktuell ausgewählte Untergruppe in eine andere Gruppe.
- **Gruppe löschen** – Löscht die aktuell ausgewählte Gruppe.
- **Bestand hinzufügen** - Fügt manuell einen Bestand hinzu. Es müssen der Bestandsname, die IP-Adresse, der Agent, die Maschinengruppe und der Bestandstyp angegeben werden.
- **Ein neues geplantes Ereignis hinzufügen** - Fügt ein **geplantes Ereignis** *(siehe 35)* hinzu.
- **Bericht erstellen** – Erstellt einen **Bericht** *(siehe 69)*.

Ansichten

Gateways und Gruppen verwenden die gleichen Ansichten.

- **Registerkarte "Bestand"** *(siehe 31)* – Diese Registerkarte wird bei Gruppen und Gateways angezeigt.
- **Registerkarte "Monitore"** *(siehe 32)* – Diese Registerkarte wird bei Gateways, Gruppen und Beständen angezeigt.
- **Registerkarte "Karte"** *(siehe 32)* – Diese Registerkarte wird bei Gruppen und Gateways angezeigt.
- **Registerkarte "Toplist"** *(siehe 34)* – Diese Registerkarte wird bei Gateways, Gruppen und Beständen angezeigt.
- **Registerkarte "Zeitpläne"** *(siehe 35)* – Diese Registerkarte wird bei Gruppen und Gateways angezeigt.
- **Registerkarte "Aktionen"** *(siehe 56)* – Diese Registerkarte wird bei Gateways, Gruppen, Beständen und Monitoren angezeigt.
- **Registerkarte "Knowledge"** *(siehe 37)* – Diese Registerkarte wird bei Gateways, Gruppen und Beständen angezeigt.
- **Registerkarte "Audit"** *(siehe 37)* – Diese Registerkarte wird bei Gateways, Gruppen, Beständen und Monitoren angezeigt.

Hinzufügen / Bearbeiten von Untergruppen

(ausgewählte Untergruppe oder Gateway) > Untergruppe hinzufügen

(ausgewählte Untergruppe) > Bearbeiten

Die Seite **Gruppe bearbeiten** konfiguriert die Eigenschaften eines Untergruppenknotens. Da es sich bei Untergruppen um "Container"-Knoten handelt, können die meisten Eigenschaften nur verwendet werden, wenn sie von Knoten auf niedrigeren Stufen geerbt werden.

- **Registerkarte "Basiseigenschaften"** *(siehe 45)* – Bei Gateways, Untergruppen und Bestand wird die Registerkarte **Basiseigenschaften** angezeigt.
- **Registerkarte "Erweitert"** *(siehe 45)* – Bei Gateways, Untergruppen, Bestand und Monitoren wird die Registerkarte **Erweitert** angezeigt.
- **Registerkarte "Authentifizierung"** *(siehe 40)* – Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.
- **Registerkarte "NOC"** *(siehe 41)* – Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.
- **Registerkarte "Markierung"** *(siehe 46)* – Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.

Registerkarte "Basiseigenschaften" – Untergruppen

Bei Gateways, Untergruppen und Bestand wird die Registerkarte ''Basiseigenschaften'' angezeigt.

Basiseigenschaften

- **Name** – Geben Sie einen Namen für die Untergruppe ein. Oft entspricht eine Untergruppe einem logischen Geschäftsbereich des Kunden.
- **Beschreibung** – Eine längere Beschreibung der Untergruppe.

Benachrichtigungs- und Wiederherstellungseinstellungen

- **Benachrichtigungsgruppe erben** – Legt die Benachrichtigungsgruppe für diesen Knoten fest. Sie können bei Gateways, Untergruppen und Bestandsknoten die Standardmeldung überschreiben, die an *Benutzergruppen* gesendet werden. Monitorknoten verwenden die Benachrichtigungsgruppe, die von ihrem übergeordneten Bestandsknoten bestimmt wird und nicht überschrieben werden kann.
- **Alarmmeldung erben** – Stellt das Format für **Alarmmeldungen** *(siehe 65)* dieses Knotens ein.
- **Aktionen erben** – Bei Markierung werden geerbte Aktionen und geerbte Wiederherstellungsaktionen in die **Registerkarte "Aktionen"** *(siehe 56)* dieses Knotens aufgenommen.

Registerkarte "Erweitert" – Gruppen

Bei Gruppen, Gateways, Bestand und Monitoren wird die Registerkarte ''Erweitert'' angezeigt.

Karten- und Standorteinstellungen

- **Karteneinstellungen erben** – Bei Markierung werden **Karteneinstellungen** *(siehe 32)* vom übergeordneten Knoten geerbt und die anderen drei Kartenoptionen sind weiterhin ausgeblendet. Deaktivieren Sie dies, um Ihre eigenen Karteneinstellungen festzulegen.
  - **Karteneinstellung** – Karten von Google verwenden. Dies ist derzeit die einzige verfügbare Option.
  - **Anzeige auf Google-Karte** – Durch Aktivieren dieser Option legen Sie fest, ob Gateways, Gruppen und Bestände auf der Karte angezeigt werden.
  - **Geografischer Standort** – Geben Sie den *Namen eines Standorts* oder die *GPS Koordinaten* in Dezimalschreibweise ein, z. B. `-33.469048, -70.642007`.
- **Zeitzone** – Monitore zeigen ihre Echtzeitgrafiken in der Ortszeit des Bestands an.
  - **Zeitzone erben** – Bei Markierung werden Zeitzoneneinstellungen vom übergeordneten Knoten geerbt. Deaktivieren Sie dies, um Ihre eigene Zeitzone anzugeben.

Kontaktinformationen

Geben Sie Kontaktinformationen für den Geschäftsbereich ein, den eine Gruppe darstellt. Wenn bei einem Bestand ein Eingriff vor Ort erforderlich ist, zeigen Sie den nächst höheren Bestand im der Monitorstruktur an, um die erforderlichen Kontaktinformationen zu erhalten.

- **Unternehmen**
- **Ansprechpartner**
- **E-Mail**
- **Telefon**
- **Mobil**
- **Fax**
- **Adresse 1**
- **Adresse 2**

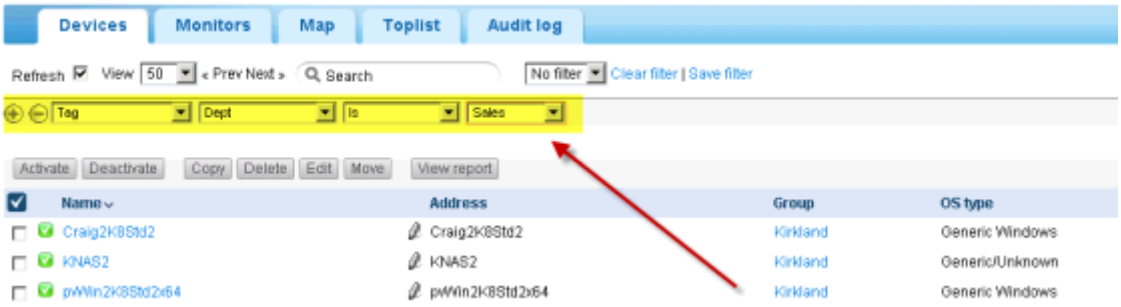
- **Zusatz**

Registerkarte "Markierungen"

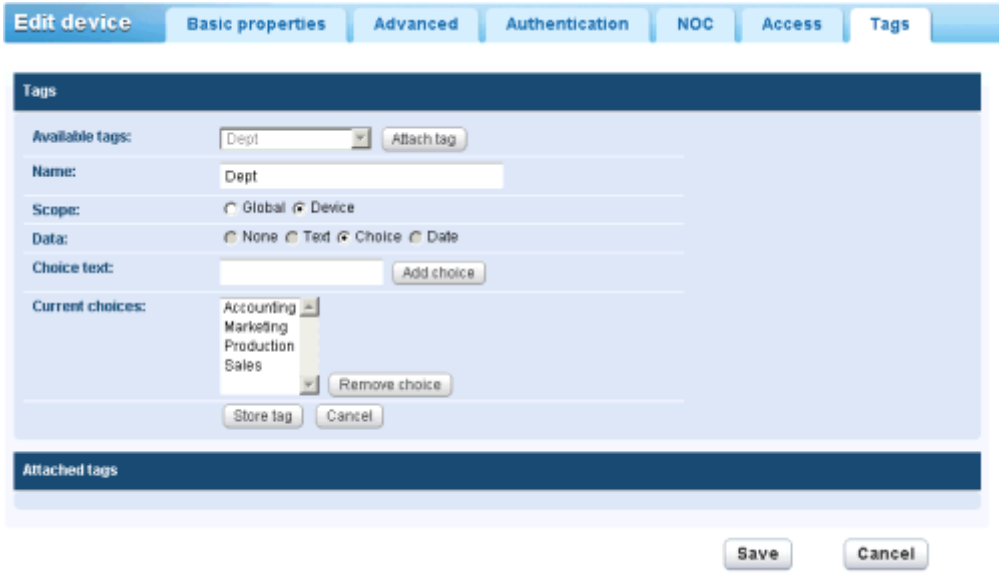
Diese Registerkarte wird bei Untergruppen und Bestand angezeigt.

Die Registerkarte **Markierungen** erstellt und bearbeitet benutzerdefinierte Markierungen und weist sie zu. Sie können eine Markierung mit einem beliebigen Knoten erstellen, der die Registerkarte "Markierung" anzeigt. Ab diesem Zeitpunkt kann die Markierung dem Knoten bzw. anderen Knoten zugewiesen werden, die dem Zuweisungsbereich der Markierung entsprechen.

Sie könnten zum Beispiel Bestand nach der Abteilung klassifizieren, zu der er gehört. Sie könnten eine `DEPT`-Markierung mit mehreren Werten erstellen: `Sales`, `Accounting`, `Marketing`, `Development`, `Manufacturing`, `Distribution`. Ansichtslisten können dann nach ihren zugewiesenen Markierungen gefiltert werden bzw. davon Berichte erstellt werden. Im Bild unten ist ein Beispiel dargestellt.



Um zum Beispiel Markierungen zu erstellen und einem Knoten in der Monitorstruktur zuzuweisen, wählen Sie eine Untergruppe oder einen Bestand aus. Klicken Sie dann **Bearbeiten** und dann auf die Registerkarte **Markierungen**.



Eine Markierung kann zwei Arten von **Scope** haben. Der Scope bestimmt, welche anderen Knotentypen die Markierung nutzen können.

- **Global** – Alle Datensatztypen können die Markierung verwenden.
- **Bestand** oder **Gruppe** – Wenn ein Bestandsknoten ausgewählt wurde, können nur andere Bestände die Markierung verwenden. Wenn ein Untergruppenknoten ausgewählt wurde, können nur andere Untergruppen die Markierung verwenden.

Sie müssen außerdem die für eine Markierung erforderliche Art der **Daten**eingabe angeben, wenn ein Benutzer eine Markierung einem Knoten zuweist.

- **Keine** – Es sind keine Daten erforderlich. Sie können zum Beispiel einfach eine Markierung mit der Bezeichnung `InMaintenance` zuweisen und so lassen.
- **Text** – Der Benutzer kann eine beliebige Art String eingeben. Bei einer Markierung mit der Bezeichnung `Note` kann der Benutzer eingeben, was er möchte.
- **Auswahl** – Der Benutzer wählt aus mehreren festen Werten einen Wert aus. Die Markierung `LicenseStatus` kann zum Beispiel auf einen der folgenden drei festen Werte eingestellt werden: `Licensed`, `Unlicensed` oder `TrialEvaluation`.
- **Datum** – Der Benutzer wählt ein Datum aus. Eine Markierung mit der Bezeichnung `RepairDueDate` könnte zum Beispiel für das erwartete Reparaturdatum eines Bestands stehen.

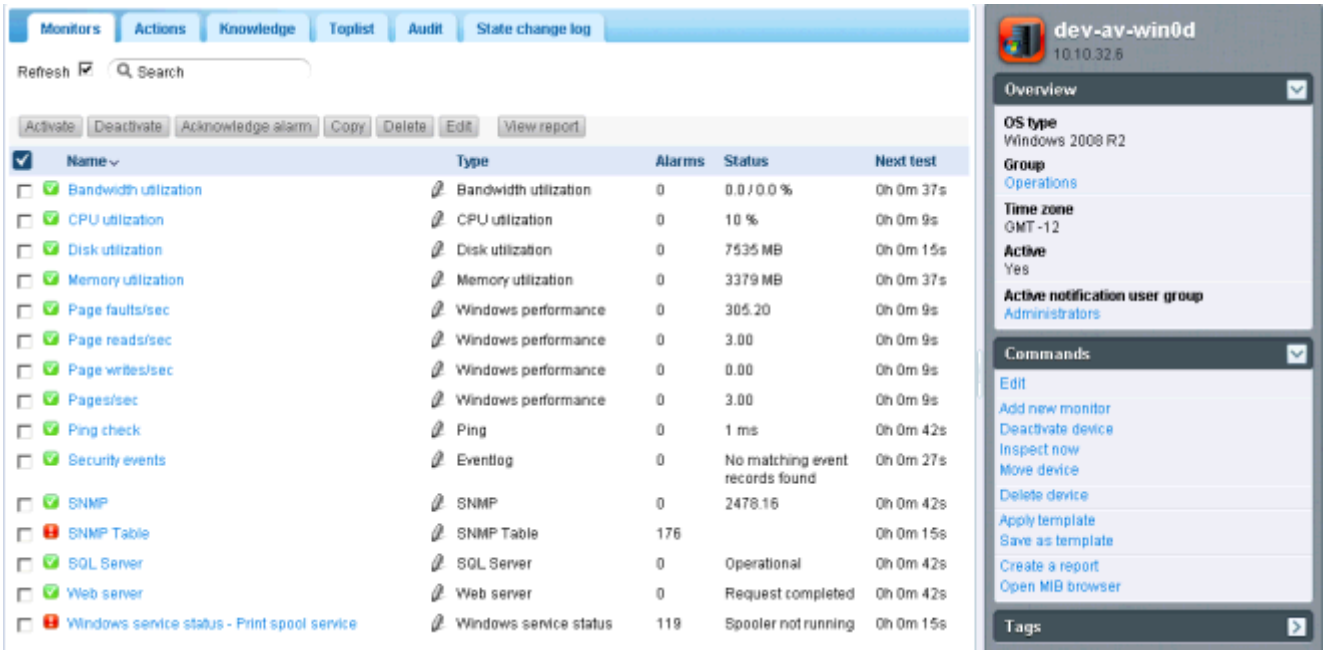
Löschen einer Markierung

- Klicken Sie auf das rote X neben einer zugewiesenen Markierung, um die Zuweisung zu löschen.

Bestand

Network Monitor Monitore *Bestände*. Ein **Bestand** repräsentiert einen Computer oder einen anderen Typ Netzwerk-Gerät, der durch eine IP-Nummer oder einen Hostnamen bezeichnet werden kann. Jeder von **Network Monitor** verwaltete Bestand wird als separater Knoten in der Monitorstruktur angezeigt. Der übergeordnete Knoten eines Bestands ist entweder ein Gateway oder eine Untergruppe. Ein ausgewählter Bestandsknoten bietet eine Listenansicht aller Monitore, die diesem Bestand zugewiesen sind.

Hinweis: Network Monitor unterstützt nicht das manuelle Hinzufügen oder Löschen von Beständen innerhalb des Network Monitor-Moduls. Ein Bestand muss von Discovery *(siehe 23)* ermittelt werden, damit Sie damit in **Network Monitor** arbeiten können.



Bestandsbefehle und Ansichten

Befehle

Diese Befehle werden angezeigt, wenn ein Bestandsknoten ausgewählt wird, unabhängig von der ausgewählten Ansichtsregisterkarte oben.

- **Bearbeiten** – Bearbeitet die **Eigenschaften** *(siehe 49)* eines Bestands.

> **Hinweis: Network Monitor unterstützt nicht das manuelle Hinzufügen oder Löschen von Bestand innerhalb des Network Monitor-Moduls.** Ein Bestand muss **von Discovery** *(siehe 23)* ermittelt werden, damit Sie damit in **Network Monitor** arbeiten können.

- **Neuen Monitor hinzufügen** – **Fügt einen neuen Monitor** *(siehe 59)* zum Bestand hinzu.
- **Bestand deaktivieren** – Deaktiviert den Bestand.
- **Jetzt prüfen** – Prüft einen Bestand, um die geeigneten **vorkonfigurierten Monitore** *(siehe 60)* für den Bestand zu bestimmen. **Jetzt prüfen** kann ausgeführt werden, wenn sich die Anmeldedaten oder die Konfiguration des Bestands geändert haben. Klicken Sie nach Ausführen von **Jetzt prüfen** auf **Neuen Monitor hinzufügen**, um die Liste der vorkonfigurierten Monitore anzuzeigen.
- **Vorlage anwenden** – Wendet eine **Bestandsvorlage** *(siehe 52)* an.
- **Als Vorlage speichern** – Speichert das Monitor-Set als **Bestandsvorlage** *(siehe 52)*.
- **Bericht erstellen** – Zeigt einen **Bericht** *(siehe 70)* an, versendet ihn per E-Mail oder veröffentlicht ihn.
- **MIB-Browser öffnen** – Zeigt die Liste der von einem Bestand unterstützten OIDs an, die mit SNMP überwacht werden können. Bei einem Bestand muss SNMP aktiviert sein, damit OIDs angezeigt werden können.

Ansichten

- **Registerkarte "Monitoring"** *(siehe 48)* – Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.
- **Registerkarte "Aktionen"** *(siehe 56)* – Diese Registerkarte wird bei Gateways, Untergruppen, Bestand und Monitoren angezeigt.
- **Registerkarte "Knowledge"** *(siehe 37)* – Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.
- **Registerkarte "Toplist"** *(siehe 34)* – Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.
- **Registerkarte "Audit"** *(siehe 37)* – Diese Registerkarte wird bei Gateways, Untergruppen, Bestand und Monitoren angezeigt.
- **Registerkarte "Statusänderungsprotokoll"** *(siehe 49)* – Diese Registerkarte wird bei Bestand und Monitoren angezeigt.

Registerkarte "Monitoring"

Diese Registerkarte wird bei Gateways, Untergruppen und Bestand angezeigt.

Aktionen

Diese Aktionen sind oben in der Listenansicht verfügbar, wenn ein oder mehrere Monitore ausgewählt werden.

- **Alarm bestätigen** – **Bestätigt Alarme** *(siehe 68)* auf ausgewählten Monitoren.
- **Aktivieren** – Aktiviert ausgewählte Monitore.
- **Deaktivieren** – Deaktiviert ausgewählte Monitore.
- **Kopieren** – Erstellt ausgewählte Monitore in ausgewählten Beständen.
- **Löschen** – Löscht ausgewählte Monitore.

- **Bearbeiten** – **Bearbeitet einen ausgewählten Monitor** *(siehe 61)*. Wenn mehrere Monitore ausgewählt sind, werden freigegebene **Standardmonitoreigenschaften** *(siehe 63)* dieser Monitore bearbeitet.
- **Bericht anzeigen** – Erzeugt einen Bericht für ausgewählten Bestand.

Tabellenspalten

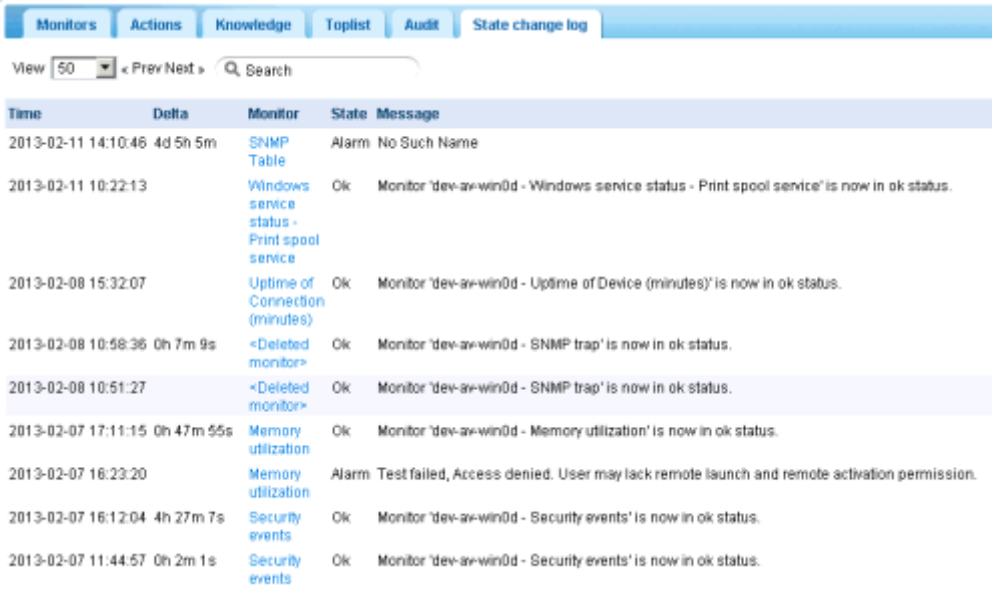
- **Name** – Der Name des Monitors.
- **Typ** – Der **Typ des Monitors** *(siehe 115)*.
- **Alarme** – Die **Alarmzählung** *(siehe 53)*. Diese Spalte wird nur bei Bestandsknoten angezeigt.
- **Status** – Das letzte vom Monitor ausgegebene Ergebnis.
- **Nächster Test** – Der Zeitpunkt, zu dem der Test das nächste Mal ausgeführt werden soll.

Registerkarte "Statusänderungsprotokoll"

Diese Registerkarte wird bei Bestand und Monitoren angezeigt.

Die Registerkarte **Statusänderungsprotokoll** wird angezeigt, wenn ein Bestandsknoten oder ein Monitorknoten ausgewählt wird. Diese Registerkarte zeigt die Statusänderungen für jeden Monitor an, der einem Bestand zugewiesen ist.

Hinweis: Bei Suchvorgängen muss auf Groß-/Kleinschreibung geachtet werden.


Monitors
Actions
Knowledge
Toplist
Audit
State change log
View 50 « Prev Next » Search
Time Delta Monitor State Message
2013-02-11 14:10:46 4d 5h 5m SNMP Table Alarm No Such Name
2013-02-11 10:22:13 Windows service status - Print spool service Ok Monitor 'dev-av-win0d - Windows service status - Print spool service' is now in ok status.
2013-02-08 15:32:07 Uptime of Connection (minutes) Ok Monitor 'dev-av-win0d - Uptime of Device (minutes)' is now in ok status.
2013-02-08 10:58:36 0h 7m 9s <Deleted monitor> Ok Monitor 'dev-av-win0d - SNMP trap' is now in ok status.
2013-02-08 10:51:27 <Deleted monitor> Ok Monitor 'dev-av-win0d - SNMP trap' is now in ok status.
2013-02-07 17:11:15 0h 47m 55s Memory utilization Ok Monitor 'dev-av-win0d - Memory utilization' is now in ok status.
2013-02-07 16:23:20 Memory utilization Alarm Test failed, Access denied. User may lack remote launch and remote activation permission.
2013-02-07 16:12:04 4h 27m 7s Security events Ok Monitor 'dev-av-win0d - Security events' is now in ok status.
2013-02-07 11:44:57 0h 2m 1s Security events Ok Monitor 'dev-av-win0d - Security events' is now in ok status.

Bearbeiten von Beständen

<ausgewählte Bestände> >Bearbeiten

Die Seite **Bestand bearbeiten** zeigt die folgenden Eigenschaftenregisterkarten an.

- **Registerkarte "Basiseigenschaften"** *(siehe 50)* – Bei Gateways, Untergruppen und Beständen wird die Registerkarte **Basiseigenschaften** angezeigt.
- **Registerkarte "Erweitert"** *(siehe 50)* – Bei Gateways, Untergruppen, Beständen und Monitoren wird die Registerkarte **Erweitert** angezeigt.
- **Registerkarte "Authentifizierung"** *(siehe 40)* – Diese Registerkarte wird bei Gateways, Untergruppen und Beständen angezeigt.
- **Registerkarte "NOC"** *(siehe 41)* – Diese Registerkarte wird bei Gateways, Untergruppen und Beständen angezeigt.

- **Registerkarte "Markierung"** *(siehe 46)* – Diese Registerkarte wird bei Gateways, Untergruppen und Beständen angezeigt.

Registerkarte "Basiseigenschaften" – Bestand

Bei Gateways, Untergruppen und Bestand wird die Registerkarte ''Basiseigenschaften'' angezeigt.

Basiseigenschaften

- **Name** – Der Name des Bestands. Diese Eigenschaft wird im **Discovery**-Modul eingestellt.
- **Adresse** – Der DNS-Name oder die IP-Adresse des Bestands. Diese Eigenschaft wird eingerichtet, wenn ein Bestand mithilfe des **Discovery**-Moduls ermittelt wird.
- **Betriebssystem** – Wählen Sie die Art des Betriebssystems des Bestands aus. Das **Betriebssystem** *(siehe 115)* bestimmt den Monitortyp, der diesem Bestand hinzugefügt werden kann. Wenn Sie nicht wissen, welchen Systemtyp der Bestand hat, oder der Systemtyp nicht verfügbar ist, wählen Sie die Option `Other/Unidentified` aus. Damit Windows-Systemmonitore ordnungsgemäß funktionieren, muss der Systemtyp unbedingt korrekt angegeben werden.
- **Bestands-Typ** – Klassifiziert den Typ des Hardwarebestands. Dies gilt nur als Referenzzweck.
- **Beschreibung** – Das Beschreibungsfeld kann verwendet werden, um den Bestand genauer zu beschreiben. Zum Beispiel den Hardwaretyp oder den physikalischen Standort.
- **Freier Text** – Das Feld für freien Text kann verwendet werden, um andere Informationen zum Bestand anzugeben und kann auch Alarmmitteilungen umfassen.

Benachrichtigungs- und Wiederherstellungseinstellungen

- **Benachrichtigungsgruppe erben** – Legt die Benachrichtigungsgruppe für diesen Knoten fest. Sie können bei Gateways, Untergruppen und Bestandsknoten die Standardmeldung überschreiben, die an *Benutzergruppen* gesendet werden. Monitorknoten verwenden die Benachrichtigungsgruppe, die von ihrem übergeordneten Bestandsknoten bestimmt wird und nicht überschrieben werden kann.
- **Alarmmeldung erben** – Stellt das Format für **Alarmmeldungen** *(siehe 65)* dieses Knotens ein.
- **Aktionen erben** – Bei Markierung werden geerbte Aktionen und geerbte Wiederherstellungsaktionen in die **Registerkarte "Aktionen"** *(siehe 56)* dieses Knotens aufgenommen.

Registerkarte "Erweitert" – Bestand

Bei Gateways, Untergruppen, Bestand und Monitoren wird die Registerkarte ''Erweitert'' angezeigt.

Erweitert

- **Aktiv** – Bei Markierung wird der Bestand als aktiv angesehen. Aktive Bestände testen ihre Monitore. Diese Option ist standardmäßig markiert.
- **SSH2-Verbindungsfreigabe** – Bei Markierung werden dauerhafte SSH2-Verbindungen für diesen Bestand aktiviert. Normalerweise wird nur eine Verbindung geöffnet und dann auf allen Monitoren freigegeben, die SSH2 bei diesem Bestand verwenden. Dadurch werden die Ergebnisse der SSH2-Verbindungsfreigabe bei mehreren Logins auf dem SSH-Server deaktiviert; dies kann jedoch bei Verbindungsproblemen hilfreich sein.
- **Überprüfung aktivieren** – Aktiviert die automatische Überprüfung auf diesem Bestand. Normalerweise führt **Network Monitor** eine Inventarisierung aller Bestände regelmäßig durch, um Hardware und angehängte Bestände zu ermitteln.
- **WMI verwenden** – Wenn ein Bestand vom Systemtyp Windows ist, verwenden die folgenden Monitortypen WMI, wenn die Bestandsmarkierung **WMI verwenden** aktiviert ist. Wenn Sie Probleme mit diesen Monitortypen haben, versuchen Sie, dieses Kontrollkästchen zu deaktivieren.
  - **WMI-Abfragemonitor** *(siehe 152)* – Verwendet immer WMI.

- **Active Directory-Monitor** *(siehe 117)* – Verwendet immer WMI.
- **Bandbreitenauslastungsmonitor** *(siehe 118)*
- **CPU-Auslastungsmonitor** *(siehe 120)*
- **Plattenauslastungsmonitor** *(siehe 124)*
- **Ereignisprotokollmonitor** *(siehe 126)*
- **Speicherauslastungsmonitor** *(siehe 133)*
- **Auslagerungsdateiauslastungs-Monitor** *(siehe 146)*

> **Hinweis:** Weitere Informationen finden Sie unter **Windows-Verwaltungsinstrumentation (WMI)** *(siehe 195)*.

Karten- und Standorteinstellungen

- **Karteneinstellungen erben** – Bei Markierung werden **Karteneinstellungen** *(siehe 32)* vom übergeordneten Knoten geerbt und die anderen drei Kartenoptionen sind weiterhin ausgeblendet. Deaktivieren Sie dies, um Ihre eigenen Karteneinstellungen festzulegen.
  - **Karteneinstellung** – Karten von Google verwenden. Dies ist derzeit die einzige verfügbare Option.
  - **Anzeige auf Google-Karte** – Durch Aktivieren dieser Option legen Sie fest, ob Gateways, Gruppen und Bestände auf der Karte angezeigt werden.
  - **Geografischer Standort** – Geben Sie den *Namen eines Standorts* oder die *GPS Koordinaten* in Dezimalschreibweise ein, z. B. `-33.469048, -70.642007`.
- **Zeitzone** – Monitore zeigen ihre Echtzeitgrafiken in der Ortszeit des Bestands an.
- **Zeitzone erben** – Bei Markierung werden Zeitzoneneinstellungen vom übergeordneten Knoten geerbt. Deaktivieren Sie dies, um Ihre eigene Zeitzone anzugeben.

Einstellungen von Bestandsabhängigkeit

- **Abhängigkeit erben –** Diese Einstellung legt die **Abhängigkeit** *(siehe 52)* des aktuell markierten Knotens an einem bzw. mehreren Monitoren fest. Bei Markierung erbt dieser Knoten seine Abhängigkeit vom übergeordneten Knoten. Wenn dies deaktiviert ist, können Sie eine Abhängigkeit ausgehend von einem anderen Satz von Monitoren *innerhalb derselben Gateway-Verzweigung der Monitorstruktur* festlegen. Alternativ können Sie keine Monitore festlegen, um so sicherzustellen, dass dieser Knoten keine Abhängigkeiten hat.
- **Abhängigkeitsmonitor auswählen/Ausgewählte Monitore** – Geben Sie Text ein um die Namen der Monitore in der Liste **Abhängigkeitsmonitor auswählen** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie ein oder mehrere Monitore in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um die Monitore der Liste **Ausgewählte Gruppen** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielmonitoren zu suchen. Um einen Monitor zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.

Einfache Wartung

Mit diesen Einstellungen kann eine Wartungsperiode für einen *einzelnen* Bestand schnell angegeben werden.

> **Hinweis:** Verwenden Sie Network Monitor > Zeitpläne > **Bestandswartung** *(siehe 93)*, um die Wartungspläne für *mehrere* Bestände anzugeben.

- **Startzeit / (Endzeit)** – Der Zeitraum am Tag, in dem dieser Bestand zu Wartungszwecken inaktiv ist.
- **Wochentag** – Die Tage der Woche, an denen dieser Bestand zu Wartungszwecken inaktiv ist.
- **Wartungsmodus** – Hält den Test während der Wartung an. Dies ist der einzig verfügbare Bestand während einer Wartungsperiode.

Testen von Abhängigkeiten

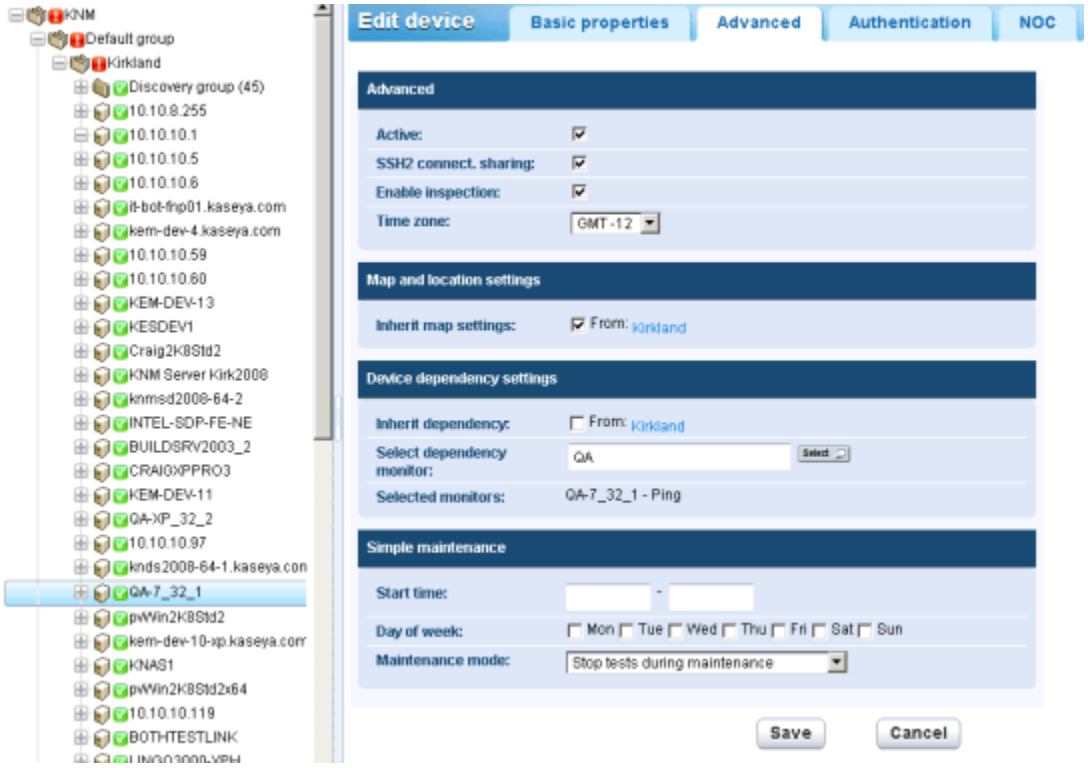
Abhängigkeiten werden mit der Registerkarte Erweitert *(siehe 50)* eines Bestandsknotens konfiguriert.

Der Benachrichtigungsstaus eines Monitors kann vom Benachrichtigungsstatus eines *beliebigen Knotens abhängig gemacht werden, der Mitglied desselben Gateways ist*.

Stellen Sie sich die Überwachung eines Routers für ein einzelnes Netzwerk vor. Wenn der Router ausfällt, ändert sich der Monitor, den Sie zum Testen dieses Routers eingerichtet haben, zuerst in den Status *Fehlgeschlagen*, dann in den Status *Alarm*. Unglücklicherweise hängen alle anderen Bestände in diesem Netzwerk von diesem Router ab. Wenn sich der Router nicht verbinden kann, so schlägt zwangsläufig auch die Verbindung aller davon abhängigen Bestände fehl. Dadurch werden für einen ganzen Zweig in der Monitorstruktur Fehler berichtet, obwohl das Problem eigentlich nur bei einem Bestand vorliegt. An diesem Punkt stören die abhängigen Bestände nur. Mit Abhängigkeitsbeziehungen können Sie verhindern, dass **Network Monitor** eine Kaskade unnötiger *Alarm*status auslöst, wenn bereits ein *Alarm*status für einen einzelnen kritischen Monitor denselben Zweck erfüllt.

Ein anderes Beispiel wäre, alle Monitore bei einem einzelnen Bestand vom **Ping-Check**-Monitor abhängig zu machen. Wenn die Netzwerkverbindung des Bestands fehlschlägt, wird nur ein Alarm für den **Ping-Check** erstellt, aber nicht für alle anderen Monitore, die diesem Bestand zugewiesen sind.

Klicken Sie für ein beliebiges Gateway, eine Untergruppe oder einen Bestandsknoten auf **Bearbeiten** und klicken Sie dann auf die Registerkarte **Erweitert**. Wählen Sie mit **Einstellungen von Bestandsabhängigkeit** den Monitor aus, von dem dieser Knoten abhängen soll. Alle Nachfolger dieses Knotens, für die Vererbung eingestellt ist, hängen von dem Monitor ab, den Sie ausgewählt haben.



Bestandsvorlagen

Bestandsvorlagen werden mit Network Monitor > Einstellungen > Bestandsvorlagen konfiguriert.

Einen Monitor gleichzeitig für tausend Bestände zu konfigurieren, ist nicht praktikabel. Konfigurieren

Sie stattdessen ein *Monitor-Set* mithilfe einer **Bestandsvorlage** *(siehe 107)* und wenden Sie dann die Bestandsvorlage auf den entsprechenden Bestand an. Sie sollten für jeden Bestandstyp, den Sie verwalten, eine Bestandsvorlage haben.

System und benutzerdefinierte Bestandsvorlagen

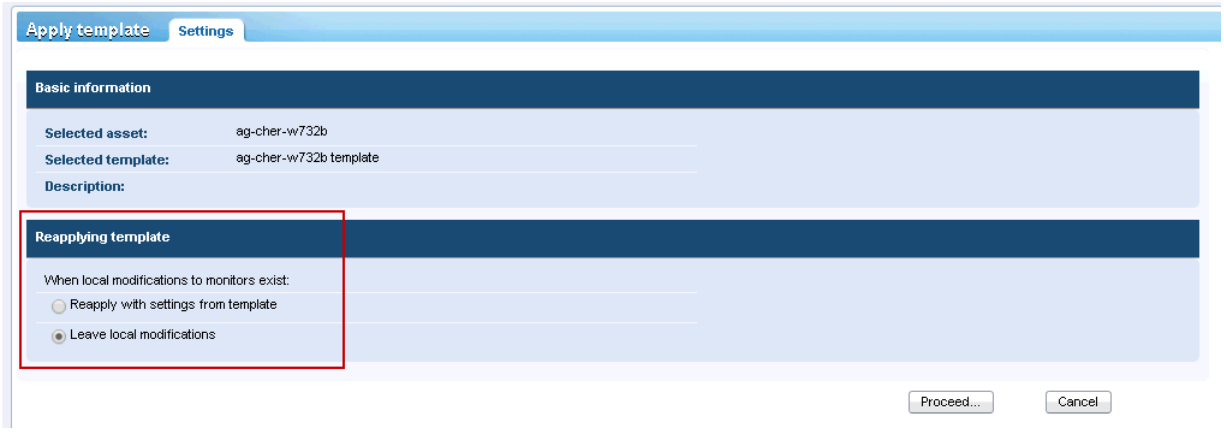
Viele Bestandsvorlagen werden mit **Network Monitor** bereitgestellt. Diese können angewendet, jedoch nicht bearbeitet werden. Sie können auch Ihre eigenen *benutzerdefinierten* Bestandsvorlagen konfigurieren, indem Sie einen Bestand mit den von Ihnen benötigten Monitoren konfigurieren und anschließend auf den Befehl **Als Vorlage speichern** klicken.

Anwenden von Bestandsvorlagen auf Bestände

Nachdem Sie eine Bestandsvorlage konfiguriert haben, müssen Sie nur noch einen Bestand auswählen und die Option **Vorlage anwenden** anklicken. Wählen Sie dann die Bestandsvorlage aus. Alle Monitore in der Bestandsvorlage werden dem ausgewählten Bestand zugewiesen und beginnen mit der Datenrückgabe. Bei Bedarf können Sie die Einstellungen von Monitoren anpassen, die durch eine Bestandsvorlage zugewiesen wurden.

Erneute Anwendung von Bestandsvorlagen

Bestände bleiben mit der Bestandsvorlage *verknüpft*, wenn die Monitore zugewiesen sind. *Änderungen an einer Bestandsvorlage werden nicht automatisch auf verknüpfte Bestände verteilt.* Sie müssen die geänderte Vorlage erneut auf jeden Bestand anwenden. Bei erneutem Anwenden einer geänderten Vorlage auf Bestände haben Sie die Option, bestandsspezifische Einstellungen bei ausgewählten Beständen zu überschreiben oder unverändert zu lassen.



Trennen von Bestandsvorlagen

Sie können einen Bestand von einer Vorlage trennen. Wenn Sie eine Bestandsvorlage trennen, sind die Monitore weiterhin dem Bestand zugewiesen.

Monitore

Ein **Monitor** prüft eine spezifische Funktion in einem Bestand. Die meisten Monitore sind in der Lage,

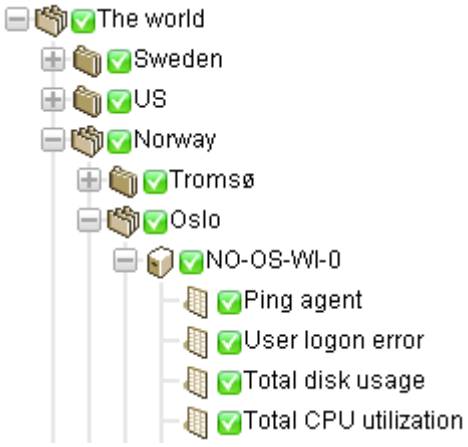
mehrere statistische Daten zu Berichtszwecken zu sammeln. Wenn ein Monitor nacheinander eine bestimmte Anzahl von Ausfällen aufweist, tritt er in einen *Alarmstatus* ein und führt eine Reihe von **Aktionen** *(siehe 56)* durch.

Der Benachrichtigungsstatus jedes Monitors wird, zusammen mit allen anderen aktiven Monitoren, bis auf die oberste Stufe der Monitorstruktur gemeldet. Wenn Sie hunderte oder tausende Monitore verwalten, können Sie mit dieser Funktion schnell den einzelnen Monitor ausfindig machen, der fehlgeschlagen ist.

Alarmstatusfortschritt

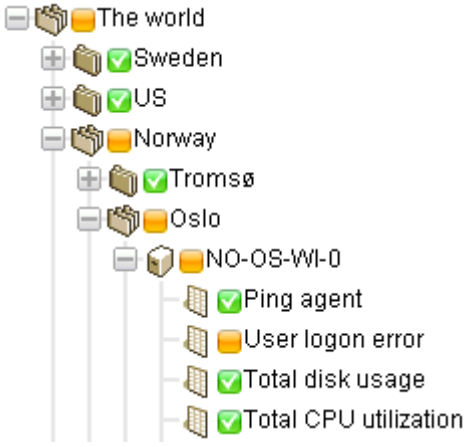
Status "OK"

Bei Normalbetrieb wird, wenn sich der Monitor im Status *OK* befindet, ein grünes Statussymbol neben dem Monitor in der Monitorstruktur angezeigt. Hier sehen Sie, wie die Monitorstruktur aussieht, wenn alle Monitore den Status *OK* haben.



Status "Fehlgeschlagen"

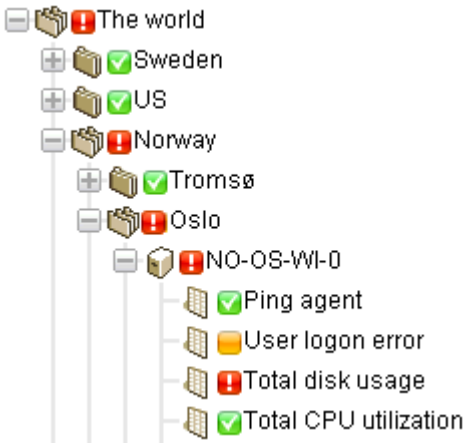
Wenn bei einem Monitor der Test fehlschlägt, so ändert sich sein Status in *Fehlgeschlagen* und neben dem Monitor wird in der Monitorstruktur ein orangefarbenes Statussymbol angezeigt. Der Status *Fehlgeschlagen* hat Vorrang vor dem Status *OK*. In diesem Fall wird das Symbol bis auf die oberste Stufe der Monitorstruktur gemeldet.



Alarmstatus

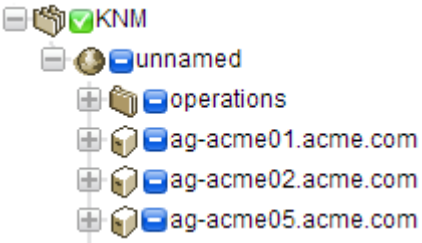
Wenn bei einem Monitor die Tests immer wieder fehlschlagen, so ändert sich sein Status in *Alarm* und neben dem Monitor wird in der Monitorstruktur ein rotes Statussymbol angezeigt. Die Anzahl der Tests, die erforderlich ist, damit ein Monitor in den Status *Alarm* versetzt wird, – auch bekannt als

Alarmzählung – ist bei den meisten Monitoren auf fünf eingestellt. Dies ist die Standardeinstellung und kann verändert werden. Da der Status *Alarm* Vorrang vor dem Status *Fehlgeschlagen* und *OK* hat, wird das Symbol bis auf die oberste Stufe der Monitorstruktur gemeldet.



Status "Verbindung getrennt"

Wenn die Verbindung eines Gateways vom Server getrennt wird, wird ein besonderes Symbol angezeigt. In diesem Fall können Gateway und alle untergeordneten Knoten ihre Daten nicht an den Server melden.



In diesem Abschnitt

Monitorbefehle und Ansichten 55
Hinzufügen von Monitoren 59
Hinzufügen von vorkonfigurierten Monitoren 60
Bearbeiten von Monitoren 61
Alarmmeldungen 65
Formatvariablen 66
Bestätigen von Alarmen 68

Monitorbefehle und Ansichten

Befehle

Diese Befehle werden angezeigt, wenn ein Monitorknoten ausgewählt wird, unabhängig von der ausgewählten Ansichtsregisterkarte oben.

- **Bearbeiten** – Bearbeitet die **Eigenschaften** *(siehe 49)* eines Bestands.
- **Deaktivieren** – Deaktiviert den Monitor.
- **Kopieren** – Kopiert den Monitor auf ausgewählte Bestände.
- **Löschen** – Löscht den Monitor.
- **Bericht erstellen** – Zeigt einen **Bericht** *(siehe 70)* an, versendet ihn per E-Mail oder veröffentlicht ihn.
- **Jetzt testen** – Testet den Monitor sofort.

Ansichten

- **Registerkarte "Übersicht"** *(siehe 48)* – Diese Registerkarte wird bei Monitoren angezeigt.
- **Registerkarte "Aktionen"** *(siehe 56)* – Diese Registerkarte wird bei Gateways, Untergruppen, Bestand und Monitoren angezeigt.
- **Registerkarte "Audit"** *(siehe 37)* – Diese Registerkarte wird bei Gateways, Untergruppen, Bestand und Monitoren angezeigt.
- **Registerkarte "Statusänderungsprotokoll"** *(siehe 49)* – Diese Registerkarte wird bei Bestand und Monitoren angezeigt.
- **Registerkarte "Alarm simulieren"** *(siehe 59)* – Diese Registerkarte wird bei Monitoren angezeigt.

Registerkarte "Übersicht"

Diese Registerkarte wird bei Monitoren angezeigt.

Die Registerkarte **Übersicht** eines aktiven Monitors zeigt die letzten zurückgegebenen Daten an. Diese Ansicht hat in der Regel drei Abschnitte.

- **Monitorstatus** – Zeigt den letzten Wert und den Schwellenwert an, bei dem der Status *Fehlgeschlagen* ausgelöst wird.
- **Live-Daten** – Ein Diagramm der letzten Testwerte, die vom Monitor zurückgegeben wurden. Der Zeitraum des Diagramms wird bei Konfiguration des Monitors eingestellt.
- **Monitor-Protokoll** – Ein Protokoll aller vom Monitor zurückgegebener Testwerte.

Registerkarte "Aktionen"

Diese Registerkarte wird bei Gateways, Untergruppen, Beständen und Monitoren angezeigt.

Die Registerkarte **Aktionen** zeigt eine Reihe an Aktionen an. Aktionen werden direkt oder durch *Vererbung* definiert. Jede Aktion wird in Folge einer bestimmten *Alarmzählung* ausgeführt. Es ist möglich – und üblich – verschiedene Aktionen für dieselbe Alarmzählung zu definieren.

Hinweis: Beachten Sie, dass von *Alarmzählung* und nicht vom *Alarmstatus* gesprochen wird. Sie können eine Reihe an Aktionen mit jeder von Ihnen gewünschten *Alarmzählung* ausführen. Diese muss nicht mit der Zählung für den *Alarmstatus* übereinstimmen.

Standardmäßige Ticket-Aktion

Wenn **Network Monitor** installiert ist, ist die Aktion **Ticket** bereits dem `KNM`-Stammknoten hinzugefügt. Standardmäßig wird die Aktion **Ticket** von jedem anderen Knoten in der Monitorstruktur vererbt. Auf diese Weise können Tickets automatisch im Modul **Ticketing** oder im **Service Desk**-Modul erstellt werden.

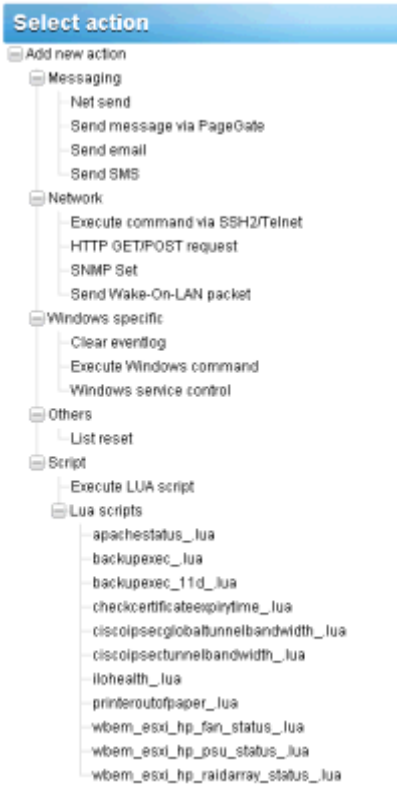
Wiederherstellungsaktionen

Möglicherweise muss ein Administrator einschreiten, um einen Bestand in einem *Alarmstatus* zu

korrigieren. Es kann auch vorkommen, dass ein Bestand vorübergehend in einen *Alarmstatus* eintritt und sich eigenständig wiederherstellt. In beiden Fällen, in denen ein Monitor wiederhergestellt wird, kann **Network Monitor** optional eine Reihe an *Wiederherstellungsaktionen* ausführen. **Wiederherstellungsaktionen werden ausgeführt, wenn ein Monitor wieder in einen ordnungsgemäßen Status wechselt.** *Wenn der Monitor wiederhergestellt wird, werden alle Wiederherstellungsaktionen, die in der Registerkarte* **Aktionen** *angezeigt werden, unabhängig von der Alarmanzahl ausgeführt.*

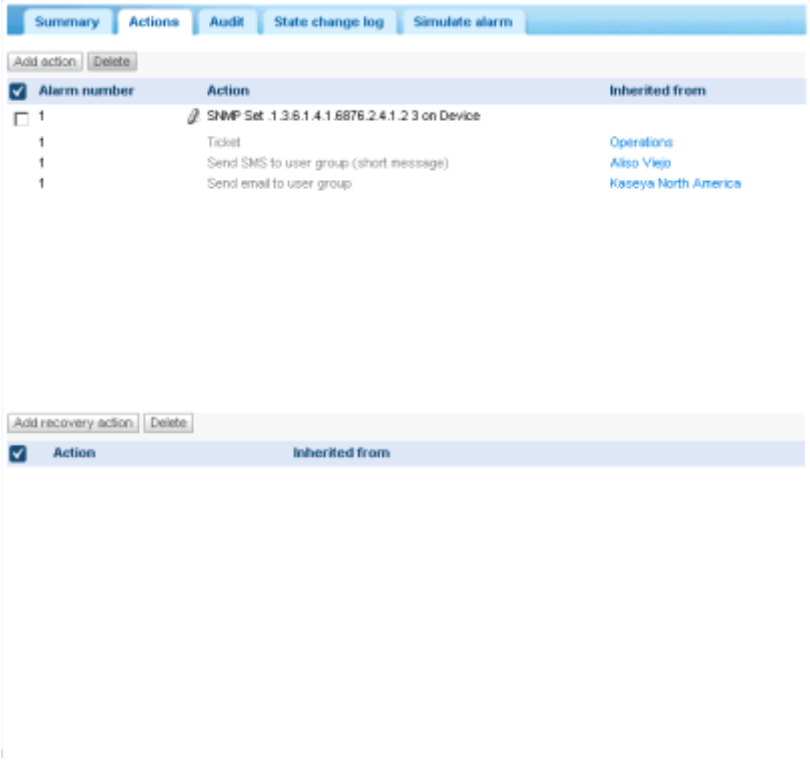
Hinzufügen von Aktionen in die Registerkarte "Aktionen"

1. Klicken Sie auf die Schaltfläche **Aktionen hinzufügen** oben auf der Registerkarte **Aktionen**.
2. Wählen Sie im mittleren Bereich eine Aktion in der Struktur **Neue Aktion hinzufügen** aus.
3. Wählen Sie den Befehl **Aktion hinzufügen** im rechten Bereich aus.
4. Bearbeiten Sie **Aktionseigenschaften** der ausgewählten Aktion. Dies ist die **Liste der Aktionen** *(siehe 155)*, die Sie auswählen können.



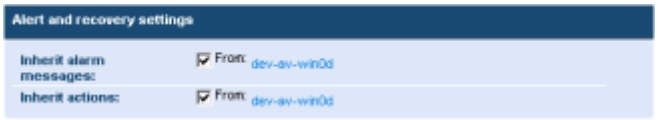
Verwalten von Hierarchien der Aktionen und Wiederherstellungsaktionen

Alle Knoten verfügen über eine Registerkarte **Aktionen**. Die Registerkarte **Aktionen** zeigt alle **Aktionen** und **Wiederherstellungsaktionen** an, die für den aktuelle ausgewählten Knoten übernommen werden. Die Spalte **Geerbt von:** kennzeichnet Aktionen, die von Knoten übergeordneter Stufen geerbt wurden. Sie können dem aktuell ausgewählten Knoten zusätzliche Aktionen und Wiederherstellungsaktionen hinzufügen. Alle Aktionen und Wiederherstellungsaktionen in dieser Registerkarte werden für alle untergeordneten Knoten übernommen, die so konfiguriert sind, dass Sie Aktionen und Wiederherstellungsaktionen erben.



Deaktivierung der Vererbung von Aktionen und Wiederherstellungsaktionen

Sie können für den aktuell ausgewählten Knoten die Vererbung von Aktionen und Wiederherstellungsaktionen deaktivieren. *Die Deaktivierung geerbter Aktionen und Wiederherstellungsaktionen wird für alle untergeordneten Knoten übernommen, die so konfiguriert sind, dass Sie Aktionen und Wiederherstellungsaktionen erben.* Im Bearbeitungsmodus – sowohl in der Registerkarte **Basiseigenschaften** als auch in der Registerkarte **Erweitert** – wird der Abschnitt **Benachrichtigungs- und Wiederherstellungseinstellungen** angezeigt. Deaktivieren Sie **Aktionen erben**, um alle geerbten Aktionen und Wiederherstellungsaktionen vom aktuell ausgewählten Knoten zu entfernen. Zeigen Sie, nachdem Sie diese Änderung gespeichert haben, erneut die Registerkarte **Aktionen** für den ausgewählten Knoten an. Sie werden sehen, dass die geerbten Aktionen und Wiederherstellungsaktionen nicht mehr angezeigt werden.



Verwalten von kundenspezifischen Aktionen und Wiederherstellungsaktionen

Eventuell ist es für Sie am einfachsten, wenn Sie benutzerdefinierte Aktionen und Wiederherstellungsaktionen auf "Kundenebene" der Monitorstruktur verwalten. Sie können zum Beispiel mit einem Gatewayknoten, der für ein einzelnes Netzwerk steht, kundenspezifische Alarmmeldungen und Alarmaktionen erstellen. Nachfolgend können diese kundenspezifischen

Einstellungen von jedem Monitor *geerbt* werden, der sich unter dem Gatewayknoten in der Monitorstruktur befindet.

Aktionen auf Gateways

Aktionen funktionieren bei Monitoren, die einem Gateway zugewiesen sind, etwas anders. Die folgenden Aktionen werden immer auf dem Server ausgeführt:

- `Send email`
- `Send SMS`
- `Paging via Pagegate`

Alle anderen Aktionen werden auf dem Gateway ausgeführt.

Registerkarte "Alarm simulieren"

Diese Registerkarte wird bei Monitoren angezeigt.

Die Registerkarte **Alarm simulieren** erzeugt einen Bericht, in dem beschrieben wird, was geschieht, wenn ein bestimmter Monitor in den *Alarmstatus* wechselt. Für eine bessere Nachvollziehbarkeit der Alarmeskalation in **Network Monitor** enthält der Bericht ausführliche Informationen zum Fortschritt der Eskalation. Die im Bericht genannte Zeit bezieht sich auf den ersten erzeugten Alarm.

In der folgenden Abbildung sehen Sie einen Beispielbericht, der von der **Alarm simulieren**-Funktion für einen `Free disk space`-Monitor mit zugewiesenen Standardaktionen erzeugt wurde.

Hinweis: Die **Alarm simulieren**-Funktion funktioniert nicht ordnungsgemäß, wenn der Systemadministrator alle Aktionen deaktiviert hat.

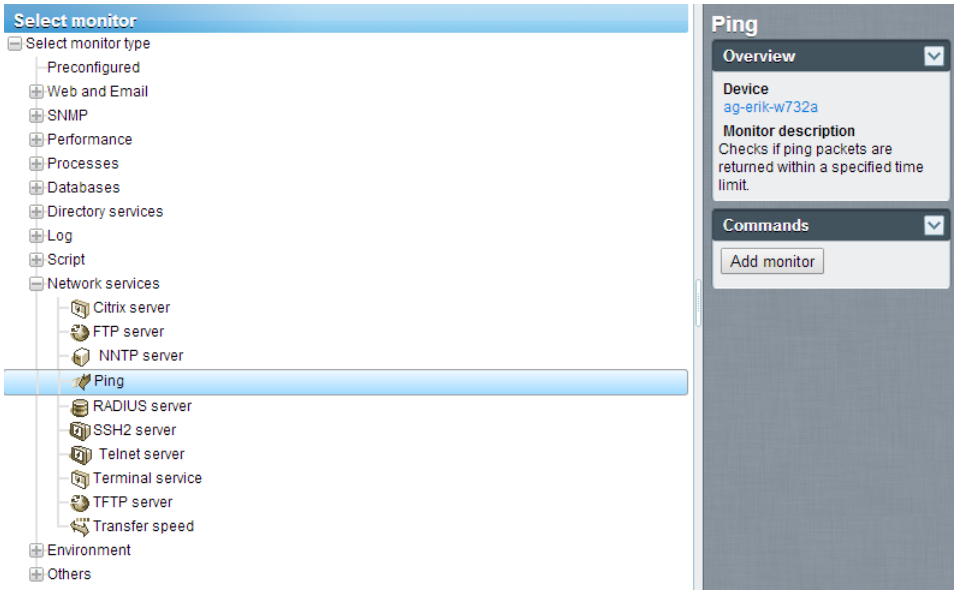
Hinzufügen von Monitoren

<ausgewählter Bestand > >Neuen Monitor hinzufügen

So fügen Sie einen Monitor zu einem Bestand hinzu:

1. Wählen Sie einen Bestandsknoten in der Monitorstruktur aus.
2. Wählen Sie den Befehl **Neuen Monitor hinzufügen**.

- Es wird eine Liste der **Monitortypen** *(siehe 115)* angezeigt, über 40 und mehr. Weitere Informationen dazu, welche Betriebssysteme welche Monitore unterstützen, finden Sie unter **Monitorreferenz** *(siehe 115)*.



3. Wählen Sie eine Kategorie und einen Monitortyp aus.
4. Wählen Sie den Befehl **Monitor hinzufügen**.
5. Konfigurieren Sie den Monitor durch **Bearbeiten der Eigenschaftsregisterkarten des Monitors** *(siehe 61)*.

> **Hinweis: Das Hinzufügen von vorkonfigurierten Monitoren** *(siehe 60)* geht sogar noch schneller!

Hinzufügen von vorkonfigurierten Monitoren

Network Monitor kann die geeigneten *vorkonfigurierten Monitore* für einen Bestand bestimmen. Normalerweise fügen Sie vorkonfigurierte Monitore direkt hinzu, nachdem ein neuer Bestand ermittelt wurde. Es wird auch empfohlen, wenn sich die Anmeldedaten oder die Konfiguration des Bestands geändert haben.

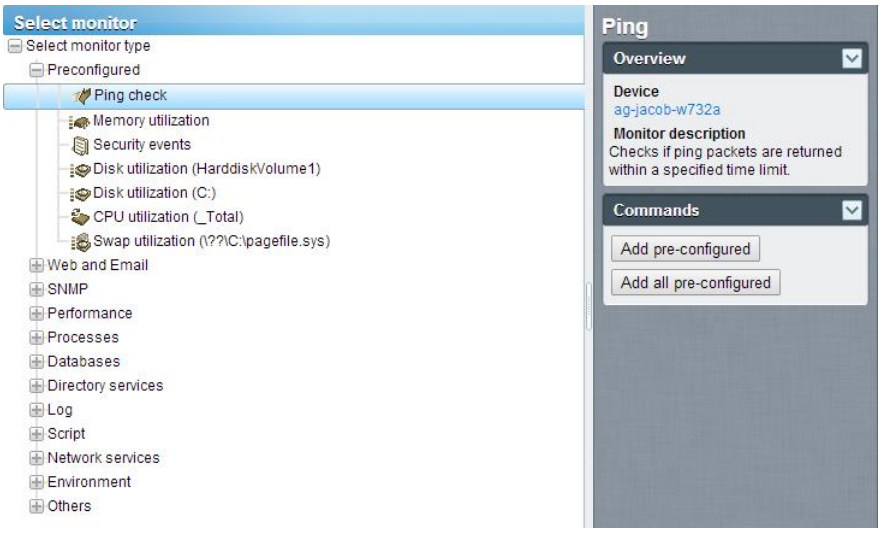
So fügen Sie vorkonfigurierte Monitore zu einem Bestand hinzu:

1. Klicken Sie auf den Befehl **Jetzt prüfen** für den Bestand. Warten Sie, bis die Überprüfung abgeschlossen ist.

   > **Hinweis:** Sie können **Jetzt prüfen** auch bei *mehreren Beständen gleichzeitig* mithilfe der Option Mehr > **Jetzt prüfen** in der Registerkarte **Bestand** *(siehe 31)* ausführen.

2. Klicken Sie auf **Neuen Monitor hinzufügen**, um die Liste der vorkonfigurierten Monitortypen anzuzeigen.
3. Klicken Sie auf einen der **vorkonfigurierten** Monitortypen in der Liste.

4. Klicken Sie entweder auf den Befehl **Vorkonfigurierten hinzufügen** oder auf den Befehl **Alle vorkonfigurierten hinzufügen**.



Bearbeiten von Monitoren

`<ausgewählter Monitor> > Bearbeiten`

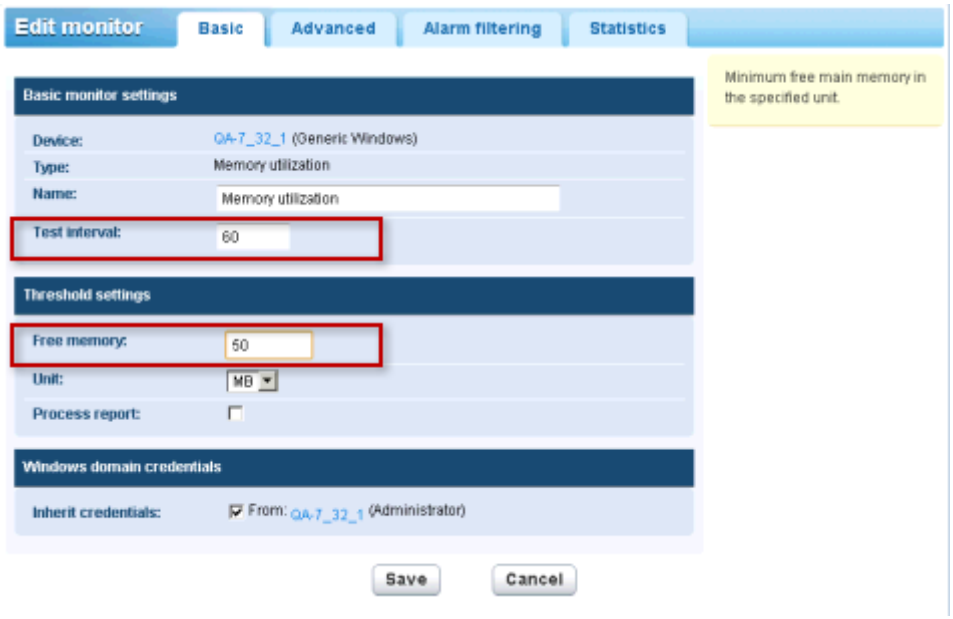
Die Registerkarte **Monitor bearbeiten** stellt die Eigenschaften von Beständen zugewiesenen Monitoren ein.

- **Registerkarte "Grundlegend"** *(siehe 63)* – Diese Registerkarte wird bei Monitoren angezeigt.
- **Registerkarte "Erweitert"** *(siehe 63)* – Bei Gateways, Untergruppen, Bestand und Monitoren wird die Registerkarte **Erweitert** angezeigt.
- **Registerkarte "Alarmfilterung"** *(siehe 64)* – Diese Registerkarte wird bei Monitoren angezeigt.
- **Registerkarte "Statistiken"** *(siehe 64)* – Diese Registerkarte wird bei Monitoren angezeigt.

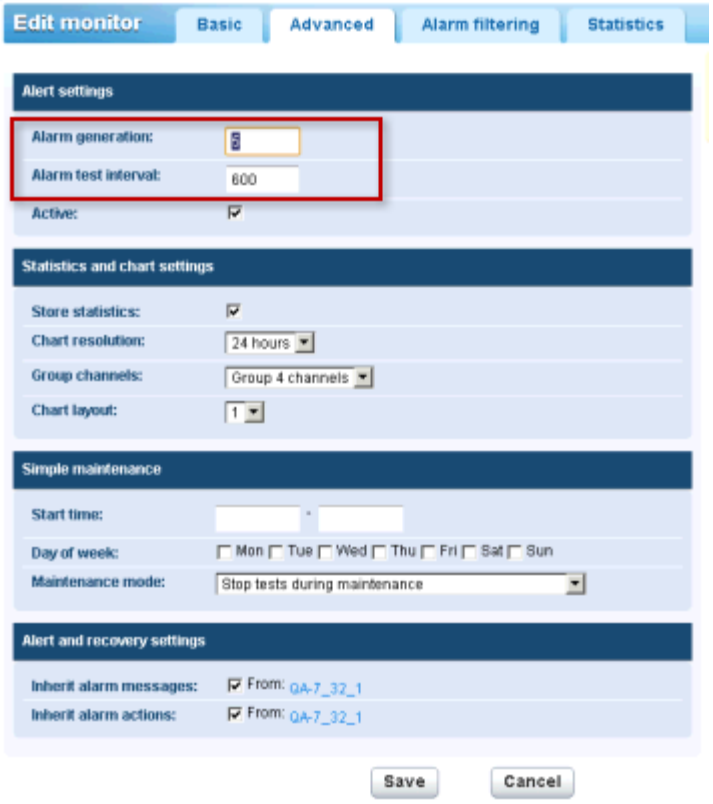
Beispiel

Im Folgenden wird erklärt, welche Eigenschaften Sie einrichten können, wenn Sie den `Performance > Memory utilization`-Monitor auswählen.

Hinweis: Bei den meisten Monitoren werden die folgenden *Standardmonitoreinstellungen* angezeigt. Siehe **Monitorreferenz** *(siehe 115)* für *monitorspezifischen Einstellungen*.



- Der Wert **Testintervall** im Abschnitt **Basiseigenschaften** zeigt an, wie viel Zeit zwischen zwei Tests verstreichen muss, *bis der erste Alarm erzeugt wird*.
- Der Abschnitt **Schwellenwerteinstellung** gibt den **freien Speicher** an, der mindestens für den Monitor erforderlich ist, wie in den Quickinfos beschrieben.



- Der Wert **Alarmerzeugung** gibt die Mindestanzahl von *aufeinanderfolgenden* Tests an, die fehlschlagen müssen, damit ein Alarm erzeugt wird.
- Der Wert **Alarmtestintervall** zeigt an, wie viel Zeit zwischen zwei Tests verstreichen muss, *nachdem der erste Alarm erzeugt wurde*. Dieses Intervall ist normalerweise sehr viel länger als das **Testintervall**, damit Sie Zeit für eine Reaktion auf den ursprünglichen Alarm haben.
- Nach der ersten Alarmzählung steigert der nächste, darauffolgende Test, der fehlschlägt, die Alarmzählung um eins.
- Wie in **Monitorstatusfortschritt** *(siehe 53)* beschrieben:
  - Wenn beim ersten Mal bei einem Monitor der Test fehlschlägt, wird das Warnsymbol neben dem Monitor in der Monitorstruktur angezeigt.
  - Wenn die Anzahl der fehlgeschlagenen Tests – die *Alarmzählung* – der Zahl im Feld **Alarmerzeugung** entspricht, tritt der Monitor in den Status *Alarm* ein. Neben dem Monitor wird in der Monitorstruktur ein Alarmsymbol angezeigt.
  - Der Monitor bleibt in seinem Alarmstatus, bis *eins* der folgenden Ereignisse eintritt:
    - ✓ Der Test schlägt in einer Serie aufeinanderfolgender Tests mindestens einmal nicht fehl.
    - ✓ Der Alarm wird von einem Benutzer bestätigt. Ein bestätigter Alarm bedeutet, dass ein Benutzer ihn erkannt hat und entsprechend handelt, um ihn zu beheben.
    - ✓ Der Monitor wird bearbeitet.

Registerkarte "Grundlegend" – Monitore

Diese Registerkarte wird bei Monitoren angezeigt.

Hinweis: Bei den meisten Monitoren werden die folgenden *Standardmonitoreinstellungen* angezeigt. Siehe **Monitorreferenz** *(siehe 115)* für *monitorspezifischen Einstellungen*.

Registerkarte "Grundlegend"

- **Bestand** – Der Name des Bestands.
- **Typ** – Der Typ des Monitors. Das identifizierte **Betriebssystem** *(siehe 115)* bestimmt den Monitortyp, der einem Bestand hinzugefügt werden kann.
- **Name** – Der eindeutige Name des Monitors. Standardeinstellungen des Monitortypnamens.
- **Testintervall** – Das Intervall, das gewartet wird, wenn der letzte Test *OK* war. In der Regel ist das Intervall länger, wenn der letzte Test *Fehlgeschlagen* ist, wie mit **Alarmtestintervall** auf der Registerkarte **Erweitert** angegeben wurde.

Registerkarte "Erweitert" – Monitore

Bei Gruppen, Gateways, Bestand und Monitoren wird die Registerkarte Erweitert angezeigt.

Hinweis: Bei den meisten Monitoren werden die folgenden *Standardmonitoreinstellungen* angezeigt. Siehe **Monitorreferenz** *(siehe 115)* für *monitorspezifischen Einstellungen*.

Benachrichtigungseinstellungen

- **Alarmerzeugung** – Gibt die Mindestanzahl von *aufeinanderfolgenden* Tests an, die fehlschlagen müssen, damit ein Alarm erzeugt wird.
- **Alarmtestintervall** – Gibt an, wie viel Zeit zwischen zwei Tests verstreichen muss, *nachdem der erste Alarm wegen "Fehlgeschlagen" erzeugt wurde*. Dieses Intervall ist normalerweise sehr viel länger als das **Testintervall** auf der Registerkarte **Grundlegend**, damit Sie Zeit für eine Reaktion auf

den ursprünglichen Alarm haben. Nach der ersten Alarmzählung steigert der nächste, darauffolgende Test, der fehlschlägt, die Alarmzählung um eins.

- **Aktiv** – Bei Markierung ist der Monitor aktiv. Ein Monitor, der nicht aktiv ist, führt keine Tests durch. Diese Option ist standardmäßig markiert.

Statistiken und Grafikeinstellungen

- **Statistiken speichern** – Bei Markierung werden erfasste Daten auf dem Datenträger gespeichert.
- **Grafikauflösung** – Die von der Grafik angezeigte Dauer.
- **Gruppenkanäle** – Die Anzahl der Datenkanäle, die in einer einzelnen Grafik erlaubt sind, wenn ein Monitor mehrere Datenkanäle ausgibt. Dies ist vor allem bei Monitoren nützlich, die separate Statistikdaten für verschiedene externe Sensoren speichern, wie z. B. dem Umgebungsmonitor.

Einfache Wartung

Mit diesen Einstellungen kann eine Wartungsperiode für einen *einzelnen* Monitor schnell angegeben werden.

> **Hinweis:** Verwenden Sie Network Monitor > Zeitpläne > **Monitorwartung** *(siehe 94)*, um die Wartungspläne für *mehrere* Monitore anzugeben.

- **Startzeit / (Endzeit)** – Der Zeitraum am Tag, in dem dieser Monitor zu Wartungszwecken inaktiv ist.
- **Wochentag** – Die Tage der Woche, an denen dieser Monitor zu Wartungszwecken inaktiv ist.
- **Wartungsmodus** – Hält den Test während der Wartung an. Dies ist der einzige verfügbare Modus während einer Wartungsperiode.

Benachrichtigungs- und Wiederherstellungseinstellungen

- **Alarmmeldung erben** – Stellt das Format für **Alarmmeldungen** *(siehe 65)* dieses Knotens ein.
- **Aktionen erben** – Bei Markierung werden geerbte Aktionen und geerbte Wiederherstellungsaktionen in die **Registerkarte "Aktionen"** *(siehe 56)* dieses Knotens aufgenommen.

Registerkarte "Alarmfilterung" – Monitore

Diese Registerkarte wird bei Monitoren angezeigt.

> **Hinweis:** Bei den meisten Monitoren werden die folgenden *Standardmonitoreinstellungen* angezeigt. Siehe **Monitorreferenz** *(siehe 115)* für *monitorspezifischen Einstellungen*.

Mit dieser Registerkarte können Sie Alarmkategorien für einen Monitor herausfiltern. Wenn ein Monitor zum Beispiel wegen einer instabilen Netzwerkverbindung einen falschen Alarm erzeugt, so entfernen Sie die Markierung von **Netzwerkfehler**, um solche Fehlertypen zu ignorieren. Standardmäßig sind alle Fehlertypen aktiviert.

- **Netzwerkfehler** – Warnt bei Fehlern wegen der Netzwerkverbindungen.
- **Schwellenwertfehler** – Warnt bei Fehlern wegen der Monitorschwellenwerte.
- **Andere Fehler** – Warnt bei Fehlern wegen unklassifizierten Fehlern.

Registerkarte "Statistiken" – Monitore

Diese Registerkarte wird bei Monitoren angezeigt.

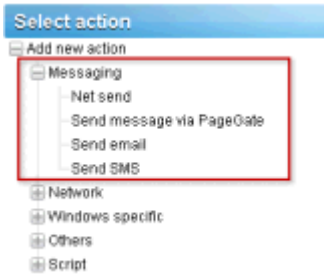
> **Hinweis:** Bei den meisten Monitoren werden die folgenden *Standardmonitoreinstellungen* angezeigt. Siehe **Monitorreferenz** *(siehe 115)* für *monitorspezifischen Einstellungen*.

Diese Registerkarte enthält die Anzeigeeinstellungen für alle Daten, die vom Monitor aufgezeichnet wurden. Bei Markierung werden die angegebenen Daten in Echtzeitgrafiken in der Monitorinformationsansicht angezeigt.

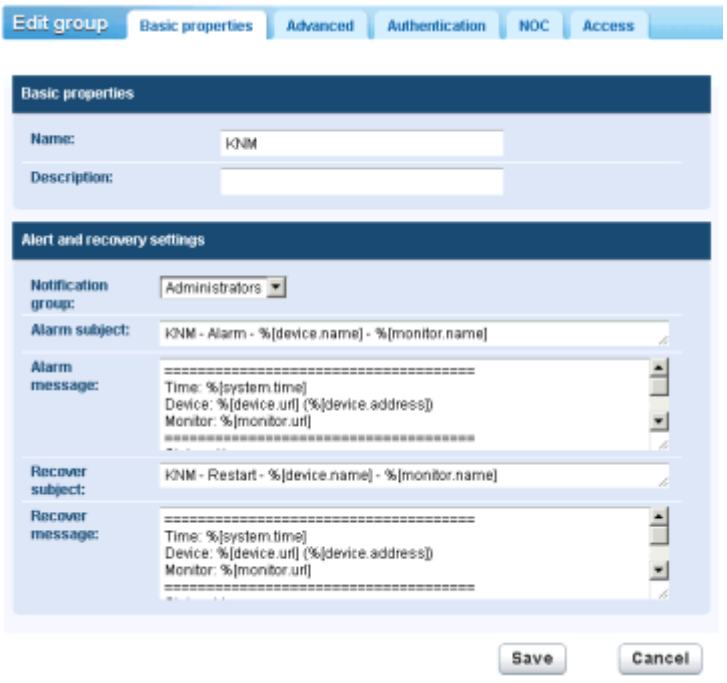
Alarmmeldungen

Alarmmeldungen können für Gateways, Untergruppen, Bestände und Monitore angegeben werden.

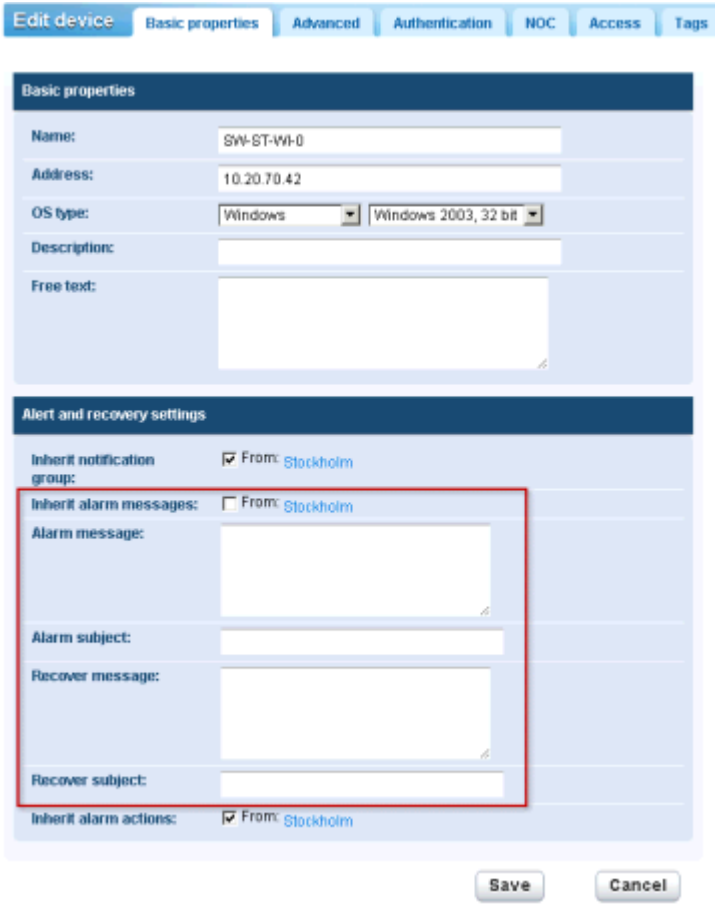
Eine der Aktionen, die durchgeführt werden können, wenn ein Alarm bei mehreren aufeinanderfolgenden Tests fehlschlägt, ist das Absenden von Meldungen.



Das Standardformat, das bei allen Meldungstypen verwendet wird, wird vom *Stammknoten* oben in der Monitorstruktur angegeben, der standardmäßig die Bezeichnung `KNM` trägt. Alle anderen untergeordneten Knoten *erben* dieses Meldungsformat, es sei denn, Sie überschreiben es. Für Aktionsmeldungen und für Wiederherstellungsmeldungen gibt es ein anderes Format. Siehe die Liste der zur Verwendung verfügbaren **Formatvariablen** *(siehe 66)*.



Um das geerbte Standardformat zu überschreiben, klicken Sie entweder auf die Registerkarte **Basiseigenschaften** oder auf die Registerkarte **Erweitert**, je nach ausgewähltem Knotentyp. Deaktivieren Sie dann das Kontrollkästchen **Alarmmeldungen erben**.



Formatvariablen

Alle ausgehenden Meldungen in **Network Monitor** können im Textteil Formatierungsvariablen enthalten. Die Formatvariablen werden aufgelöst, bevor die Meldungen verarbeitet und an die Empfänger gesendet werden. Bei den meisten dieser Formatvariablen wird auf Groß- und Kleinschreibung geachtet. Die Formatvariable `%[monitor.error]` wird zum Beispiel nur aufgelöst, wenn eine Monitoraktion einen Alarm auslöst. Dieselbe Formatvariable wird nicht aufgelöst, wenn sie in einem geplanten Ereignis **E-Mail senden** verwendet wird.

%[system.time]	aktuelle Zeit
%[system.time_hour]	24-Stunden-Format
%[system.time_hour2]	12-Stunden-Format
%[system.time_minute]	einschließlich Minuten
%[system.time_second]	einschließlich Sekunden
%[system.date]	aktuelles Datum
%[system.date_year]	aktuelles Datum mit vollständiger Jahreszahl
%[system.date_year2]	Jahreszahl ohne Jahrhundertangabe
%[system.date_month]	Monat als Zahl 01–12

%[system.date_day_of_month]	Tag des Monats 01–31
%[system.date_weekday]	0 = Sonntag, 6 = Samstag
%[system.date_day_of_year]	Tag des Jahres 1–366
%[group.name]	Name der Gruppe
%[group.path]	vollständiger Pfad der Gruppe
%[group.id]	eindeutige Gruppen-ID
%[group.url]	Verknüpfung zur Gruppe
%[group.kb_article_url]	Verknüpfung zu Artikeln der aktuellen Gruppe
%[group.company]	Gruppen-/Unternehmensname
%[group.additional]	Gruppe/Unternehmen, zusätzliche Zeile 1
%[group.additional]	Gruppe/Unternehmen, zusätzliche Zeile 2
%[group.contact]	Ansprechpartner für Gruppe/Unternehmen
%[group.email]	E-Mail-Adresse von Gruppe/Unternehmen
%[group.phone]	Telefonnummer von Gruppe/Unternehmen
%[group.cellphone]	Mobiltelefonnummer von Gruppe/Unternehmen
%[group.fax]	Faxnummer von Gruppe/Unternehmen
%[group.address1]	Adresse 1 von Gruppe/Unternehmen
%[group.address2]	Adresse 2 von Gruppe/Unternehmen
%[asset.local_time]	lokale Uhrzeit des Bestands
%[asset.name]	name
%[asset.id]	eindeutige Bestands-ID
%[asset.free_text]	
%[asset.address]	
%[asset.ip]	
%[asset.description]	
%[asset.notification_group]	
%[asset.mac]	
%[asset.url]	Verknüpfung zu Bestand
%[asset.kb_article_url]	Verknüpfung zu Artikeln des aktuellen Bestands
%[monitor.name]	
%[monitor.id]	
%[monitor.error]	
%[monitor.error2]	
%[monitor.type]	
%[monitor.current_status]	
%[monitor.time_last_ok]	
%[monitor.time_last_ok_local_time]	

%[monitor.time_last_failed]	
%[monitor.time_last_failed_local_time]	
%[monitor.dependency_status]	
%[monitor.url]	
%[user.current]	Name des Benutzers, verwendet bei Alarmbestätigung
%[user.on_duty]	Name des "diensthabenden" Benutzers, definiert nach dem Benutzerarbeitsplan
%[user.distribution_list]	Liste der Benutzer, die die E-Mail erhalten
%[system.charts]	Echtzeitgrafiken des Monitors
%[report.name]	
%[report.description]	
%[monitor.list]	verwendet bei Alarmbestätigung, Monitore, die bestätigt wurden

Bestätigen von Alarmen

Sie können einen Alarm bestätigen, indem Sie die Schaltfläche Bestätigen auswählen, die sich im oberen Bereich einer beliebigen Registerkarte für die Anzeige des Monitors auf einem Gateway, einer Untergruppe oder einem Bestandsknoten befindet.

Ein Benutzer kann den Alarmstatus von mindestens einem Monitor bestätigen, um andere Benutzer zu informieren, dass die Alarme untersucht werden. Um einen Alarm zu bestätigen, kann der Benutzer aus zwei Optionen wählen:

- `Clear alarm status` – Der Alarmstatus wird gelöscht und der Monitor kehrt zurück zum Status *OK*.

- `Deactivate the monitors` – Der Monitor wird deaktiviert. Verwenden Sie dazu ein Kontrollkästchen, um **die Monitore automatisch nach N Minuten zu reaktivieren**. Ist das Kontrollkästchen für die Reaktivierung nicht markiert, bleiben die Monitore so lange deaktiviert, bis sie manuell aktiviert werden.

Format der Bestätigungsbenachrichtigung

Das Format der Bestätigungsbenachrichtigungsmeldung wird *nicht für den gesamten Monitorbaum übernommen*. Stattdessen wird das Standardformat für Benachrichtigungen über die Registerkarte Network Monitor Einstellungen > SMS > **Standardnachrichten** *(siehe 113)* angegeben und ist für alle Knoten gültig.

> **Hinweis:** Das Thema **Formatvariablen** *(siehe 66)* führt die Formatvariablen auf, die in einer Bestätigungsbenachrichtigungsmeldung verwendet werden können.

Berichte

Network Monitor kann statistische Berichte aus aufgezeichneten Monitordaten erzeugen. Alle Berichte werden mit einem allgemeinen Satz an Designelementen, wie z. B. Grafiken, Toplists, Informationen zu Ausfallzeiten, Datentabellen, Kommentaren und Bildern erstellt. Die Gesamtgestaltung und die Farbeinstellungen des Berichts werden durch Stilvorlagen gesteuert, wodurch Sie dem fertiggestellten Bericht das Farbschema oder Logo Ihres Unternehmens hinzufügen können.

Dieser Abschnitt beschreibt, wie unterschiedliche Berichtstypen angezeigt und veröffentlicht werden können.

Anzeigen von Berichtsvorlagen

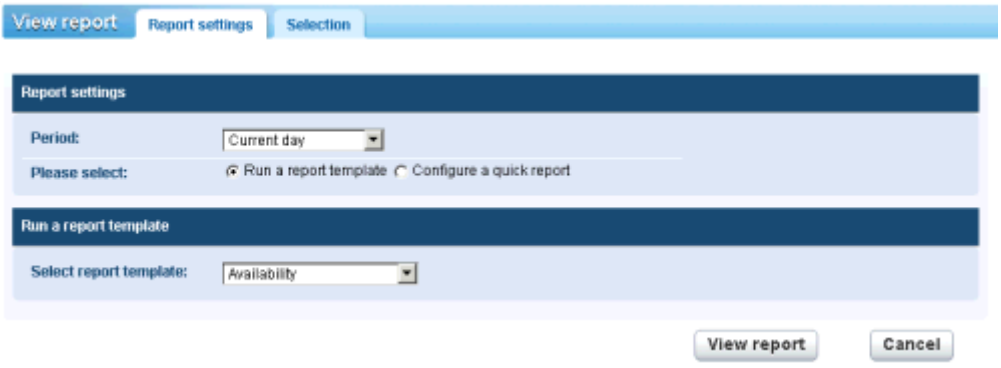
`<Knoten auswählen> >Bericht erstellen >In Browser anzeigen.`

Mit der Seite **Bericht anzeigen** können Sie zwei Berichtstypen anzeigen.

- **Berichtsvorlagen**
- **Schnellberichte**

Üblicherweise wählen Sie Gruppen, Bestände oder Monitore *zuerst* aus und anschließend den anzuzeigenden Berichtstyp.

1. Wählen Sie einen beliebigen Knoten in der Monitorstruktur aus, üblicherweise ein Gateway oder eine Untergruppe. Abhängig vom Knotentyp werden entweder Bestände oder Monitore im mittleren Bereich aufgelistet.
2. Klicken Sie auf die Schaltfläche **Bericht anzeigen** oder wählen Sie den Befehl **Bericht erstellen >In Browser anzeigen** aus, damit die Seite **Bericht anzeigen** erscheint.



Berichtseinstellungen

Die Registerkarte **Berichtseinstellungen** auf der Seite **Bericht anzeigen** zeigt drei Anfangsoptionen an:

- **Dauer** – Wählen Sie die Dauer des Berichts aus.
  - `Current day`, `week`, `month`, `quarter`, `year`
  - `Last day`, `week`, `month`, `quarter`, `year`
  - `User defined period`
  - `Offset in days`
- **Berichtsvorlage ausführen** – Wählen Sie aus einer Liste vordefinierter Berichtsvorlagen aus. **Network Monitor**ist mit einer Reihe nützlicher **Berichtsvorlagen** vorkonfiguriert. Sie können diese anpassen oder eigene erstellen. Der Datentyp und die Designelemente sind bereits in einer Berichtsvorlage ausgewählt. Sie müssen sich nur für die auszuführende Berichtsvorlage entscheiden.
- **Schnellbericht konfigurieren** – Wir empfehlen Ihnen bestimmte Monitore auszuwählen, bevor Sie diese Option markieren. In diesem Fall beinhaltet der **Schnellbericht** *(siehe 71)* standardmäßig eine Reihe kompatibler Designelemente für die von Ihnen ausgewählten Monitore. Wenn keine Monitore ausgewählt wurden, bevor diese Option markiert wurde, muss jedes Designelement einzeln manuell eingefügt werden.

Auswahl

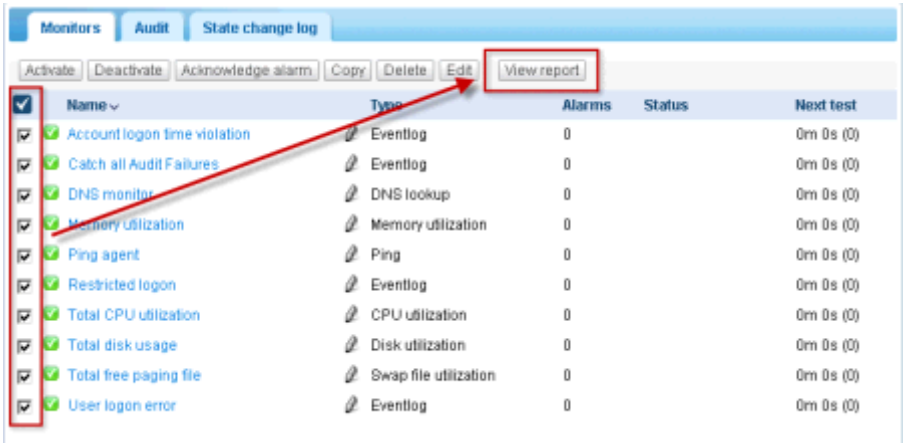
Überschreiben Sie in der Registerkarte **Auswahl** der Seite **Bericht anzeigen** die Standardauswahl für Gateway oder Untergruppe, Bestände und Monitore, die für jeden Berichtstyp ausgewählt sind.

Schnellberichte anzeigen

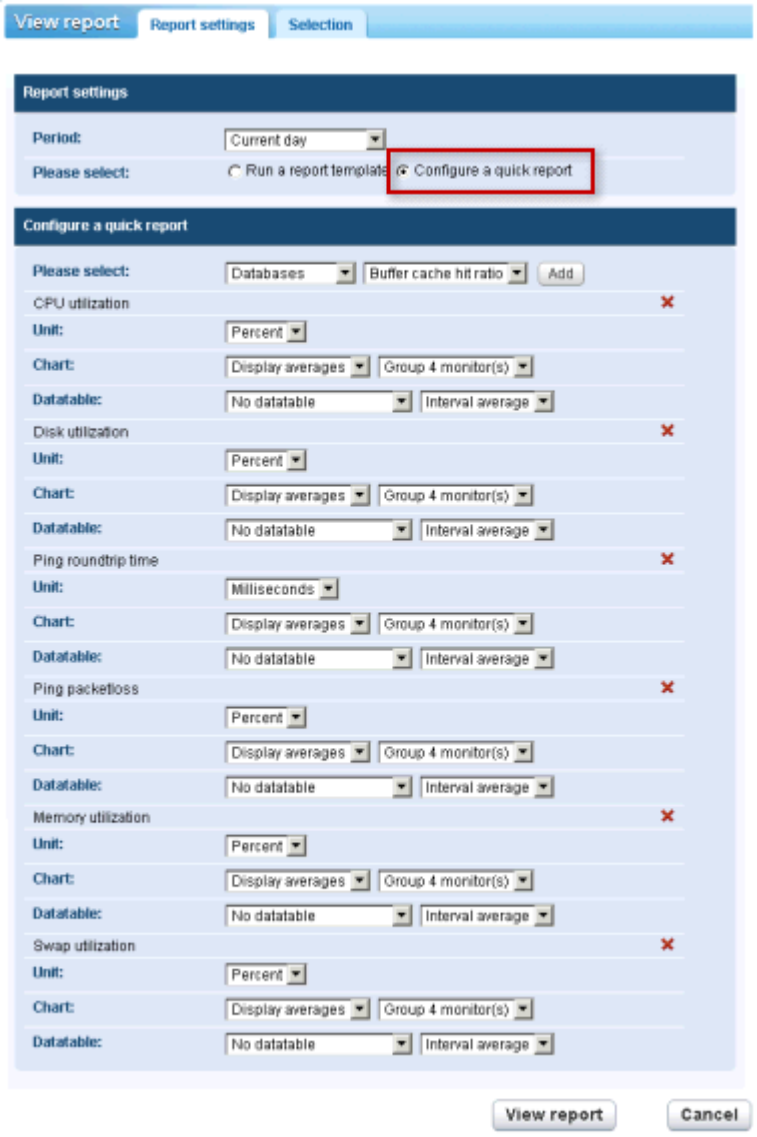
<Einen Knoten auswählen> > <Monitore auswählen> > Bericht anzeigen

Sobald Bestände verschiedenen Monitortypen zugewiesen sind, führen Sie einen **Schnellbericht** aus, um *Daten von verschiedenen Monitortypen zu vergleichen.* Wenn mehrere Bestände ausgewählt sind, werden Daten für den gleichen Monitortyp im gleichen Diagramm zusammen gruppiert.

Am schnellsten lässt sich ein Schnellbericht über die Listenansicht einer Registerkarte **Monitore** eines einzelnen Bestands konfigurieren. Wählen Sie alle Monitore für diesen Bestand auf der Registerkarte **Monitore**. Klicken Sie auf die Schaltfläche **Bericht anzeigen** oben in der Monitor-Liste.



Klicken Sie auf die Option **Einen Schnellbericht konfigurieren**. Die Registerkarte **Berichtseinstellungen** listet eine Reihe an Konfigurationsabschnitten auf, einen oder mehrere für jeden Monitortyp, den Sie zuvor ausgewählt haben.



Klicken Sie auf die Schaltfläche **Bericht anzeigen** unten in der Monitor-Liste. Monitordaten werden für jeden der Abschnitte, die auf der Registerkarte **Berichtseinstellungen** konfiguriert sind, im Diagrammformat angezeigt.

Hinweis: Um den Bericht in einer neuen Registerkarte oder einem neuen Fenster anzuzeigen, legen Sie die Dropdownliste Network Monitor > Benutzer > Eigene Einstellungen > Registerkarte ''Benutzeroberflächenoptionen'' > **Berichte anzeigen** auf `Open reports in a new window` fest.

Mit derselben Seite können Sie:

- Neue Abschnitte mithilfe der Schaltfläche **Hinzufügen** im oberen Bereich der Registerkarte **Berichteinstellungen** hinzufügen.
- Eine andere Zeit**periode** auswählen.
- Die Registerkarte **Auswahl** verwenden, um mehrere Gruppen, Bestände und Monitore auszuwählen.

Hinweis: Sie können auch die Option **Berichtsvorlage ausführen** auswählen, um einen Bericht mit einem vordefinierten Layout für die von Ihnen ausgewählten Bestände auszuführen.

Anzeigen angepasster Berichte

Angepasste Berichte sind für das Definieren von Berichten geeignet, dessen Inhalt sich nicht ändert. Ein angepasster Bericht ist auch die einzige Möglichkeit, einen Bericht zu erstellen, der Daten für unterschiedliche Zeitperioden im gleichen Bericht erhält.

Angepasste Berichte sind wie Berichtsvorlagen aufgebaut, *aber an spezifische Gruppen, Bestände und Monitore gebunden.* Aus diesem Grund werden angepasste Berichte nicht ausgeführt, indem ein Knoten im Monitorbaum zuerst ausgewählt wird. *Stattdessen erstellen Sie angepasste Berichte und führen Sie diese aus, indem Sie* Network Monitor > Berichte > **Berichte angepasst** *(siehe 79)* auswählen.

Hinweis: Da die Gestaltung und das Ausführen angepasster Berichte den Berichtsvorlagen sehr ähnlich sind, sollten Sie sich zuerst mit dem Konfigurieren von **Berichtsvorlagen** *(siehe 80)* vertraut machen. Mit angepassten Berichten stehen Ihnen zusätzliche Felder zur Verfügung, mit denen Sie Gruppen, Bestände und Monitore angeben können.

Berichte per E-Mail versenden und veröffentlichen

<Knoten auswählen> >Bericht erstellen >E-Mail oder veröffentlichen

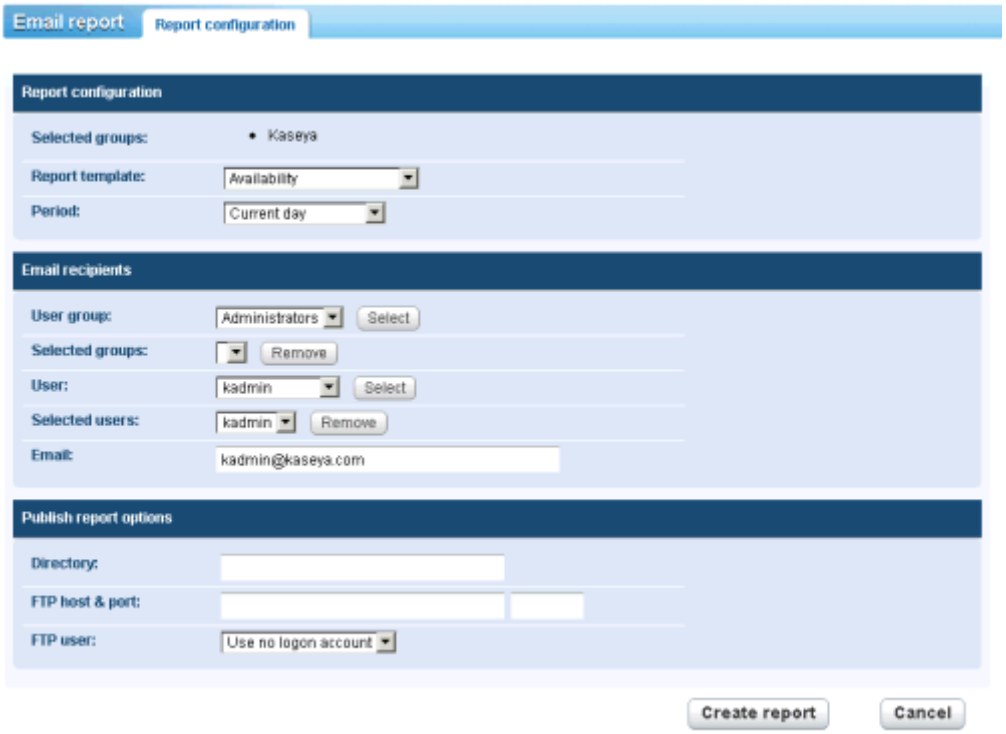
Network Monitor > Berichte > Berichte anpassen > (klicken Sie auf das Symbol)

Die Seite **E-Mail-Bericht** verteilt eine ausgewählte Berichtsvorlage oder einen angepassten Bericht als E-Mail-Anhang bzw. füllt den Speicherort einer Datei auf. Vor dem Generieren des Berichts ist eine Vorschau des Berichts nicht möglich.

Wählen Sie *zuerst* die Untergruppen, Bestände und Monitore.

1. Wählen Sie einen beliebigen Knoten in der Monitorstruktur aus, üblicherweise eine Untergruppe. Abhängig vom Knotentyp werden entweder Bestände oder Monitore im mittleren Bereich aufgelistet.

2. Klicken Sie auf die Schaltfläche **Bericht anzeigen** oder wählen Sie den Befehl Bericht erstellen > **E-Mail oder veröffentlichen** aus, um die Seite **E-Mail-Bericht** anzuzeigen.



Berichtskonfiguration

- **Ausgewählte Gruppen** – Zeigt den ausgewählten Untergruppen-Knoten an.
- **Berichtsvorlage** – Wählen Sie eine Berichtsvorlage aus.
- **Dauer** – Wählen Sie die Dauer des Berichts aus.
  - Aktueller Tag, Woche, Monat, Quartal, Jahr
  - Letzter Tag, Woche, Monat, Quartal, Jahr
  - Benutzerdefinierte Dauer
  - Verschiebung in Tagen

E-Mail-Empfänger

- **Bestände auswählen/Ausgewählte Bestände** – Geben Sie Text ein, der mit einem Teil des Namens eines Bestands übereinstimmt. Wählen Sie einen oder mehrere Bestände aus der Liste **Bestände auswählen** aus und klicken Sie auf die Schaltfläche **Hinzufügen**. Um eine oder mehrere Benutzergruppen aus **Ausgewählte Gruppen** zu entfernen, wählen Sie eine Benutzergruppe und klicken Sie auf die Schaltfläche **Entfernen**.
- **Benutzer/Ausgewählte Benutzer**– Wählen Sie einen oder mehrere VSA-Benutzer aus der Liste **Benutzer** und klicken Sie auf die Schaltfläche **Auswählen**. Um einen oder mehrere Benutzer aus der Liste **Ausgewählte Benutzer** zu entfernen, wählen Sie die Benutzer aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **E-Mail** – Geben Sie einzelne E-Mail-Adressen als Empfänger an. Trennen Sie mehrere Einträge mit einem Komma voneinander.

Optionen Bericht veröffentlichen

Anstatt einen Bericht per E-Mail zu versenden, können Sie ihn auch an einem Netzwerkspeicherort speichern.

- **Verzeichnis** – Der generierte Bericht wird in einem Netzwerkordner als HTML-Dokument veröffentlicht. Geben Sie den Pfad zu diesem Ordner an. Fügen Sie optional die folgenden Variablen für die Formatierung ein, wenn Sie den Dateinamen angeben.
  - `%[system.date]` – aktuelles vollständiges Datum
  - `%[system.date_year]` – aktuelles Jahr
  - `%[system.date_month]` – aktueller Monat
  - `%[system.date_day_of_month]` – aktueller Monatstag
  - `%[system.time]` – aktuelle vollständige Zeit
  - `%[system.time_hour]` – aktuelle Stunde
  - `%[system.time_minute]` – aktuelle Minute
  - `%[system.time_second]` – aktuelle Sekunde
- **FTP-Host & Port** – Der generierte Bericht kann auf einem FTP-Server als HTML-Dokument veröffentlicht werden. Geben Sie den Hostnamen und die Port-Nummer an. Standardeinstellungen `21`.
- **FTP-Benutzer** – Wählen Sie das Anmeldekonto, das für das Authentifizieren beim FTP-Server verwendet wird.

Planen von Berichten

Das Planen der automatischen Generierung von Berichten erfolgt über die Funktion für geplante Ereignisse. Informationen dazu, wie mit geplanten Ereignissen gearbeitet wird, finden Sie im Abschnitt **Geplante Ereignisse** *(siehe 35)*. Dokumentation für das Ereignis **Bericht erstellen** *(siehe 167)* finden Sie im Abschnitt **Referenz geplantes Ereignis**.

Kapitel 3

Informationen zum Navigationsfeld

Im Navigationsfeld für **Network Monitor** gibt es Moduleinstellungen und -Funktionen, die unabhängig von jedem Knoten im Monitorbaum sind.

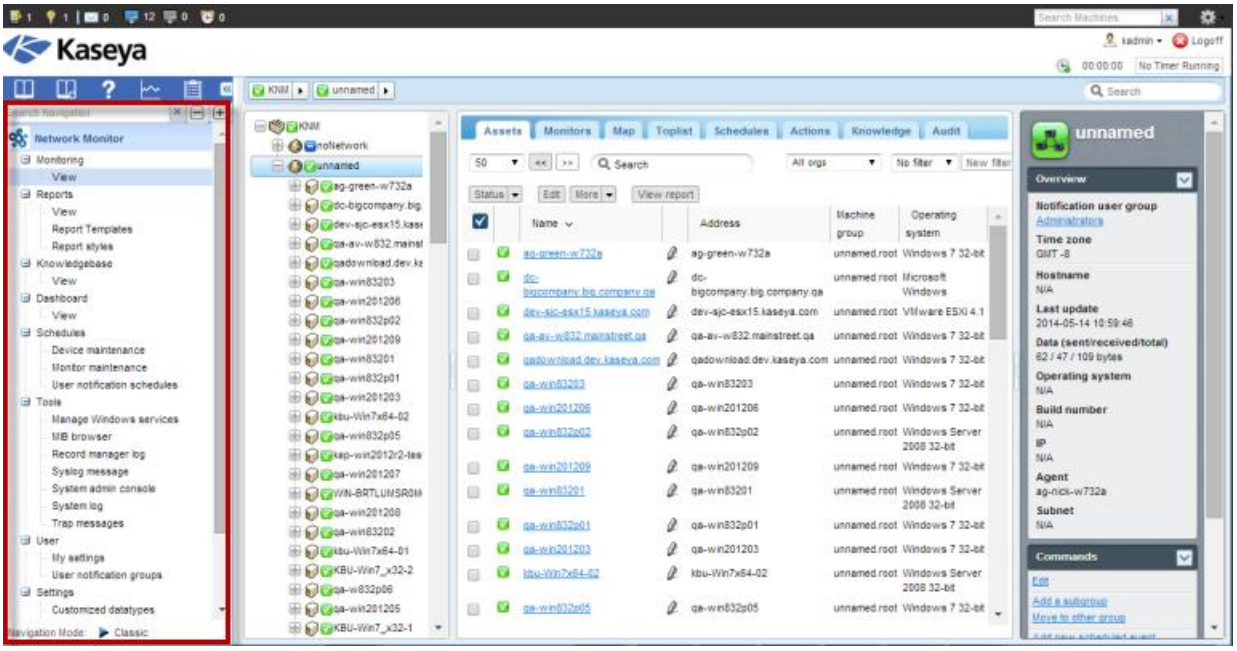
In diesem Kapitel

Überblick über das Navigationsfeld 78
Berichte angepasst 79
Berichtsvorlagen 80
Knowledge-Base-Artikel 89
Dashboard 92
Bestandswartung 93
Monitorwartung 94
Benutzerbenachrichtigungspläne 95
Liste der Windows-Dienste 96
MIB Browser 97
Datensatzmanagerprotokoll 100
Syslog-Meldung 101
Systemadministratorkonsole 102
Systemprotokoll 104
Trap-Meldungen 104
Eigene Einstellungen 104
Benutzerbenachrichtigungsgruppen 105
Angepasste Datentypen 106
Bestandsvorlagen 107
Protokolleinstellungen 108
NOC-Einstellungen 109
Weitere Systemeinstellungen 109
SMS-Einstellungen 110
Standardnachrichten 113

Überblick über das Navigationsfeld

Das Navigationsfeld von **Network Monitor** bietet unterschiedliche Inhaltsansichten und gibt Ihnen die Möglichkeit, Einstellungen auf Modulebene zu konfigurieren.

Hinweis: Das Navigationsfeld übernimmt die Funktion des ''K-Menüs'' in früheren, Standalone-Versionen von **Network Monitor**.



Diese Funktionen werden detailliert in den **Informationen zum Navigationsfeld** *(siehe 77)* ausgeführt, die in dieser Dokumentation enthalten sind. Bei Folgendem handelt es sich um eine beschreibende Zusammenfassung jeder Option des Navigationsfelds.

Funktionen	Beschreibung
Monitoring > **Ansicht** *(siehe 13)*	Wählt die **Monitoringansicht** *(siehe 13)* aus.
Berichte > **Ansicht** *(siehe 79)*	Konfiguriert benutzerdefinierte Berichte, die mit ausgewählten Knoten verbunden sind.
Berichtsvorlagen *(siehe 80)*	Konfiguriert Berichtsvorlagen, die mit allen Knoten verbunden werden können.
Berichtstile *(siehe 81)*	Konfiguriert das generelle Layout der Berichte, der Berichtsvorlagen und der benutzerdefinierten Berichte.
Knowledgebase > **Ansicht** *(siehe 89)*	Wählt die Ansicht "Knowledgebase" aus.
Dashboard > **Ansicht** *(siehe 92)*	Wählt die Ansicht "Dashboard" aus.
Bestandswartung *(siehe 93)*	Konfiguriert die Bestandswartungspläne.
Monitorwartung *(siehe 94)*	Konfiguriert Monitorwartungspläne.
Benutzerbenachrichtigungspläne *(siehe 95)*	Konfiguriert Network Monitor Benutzerarbeitspläne.
Management Windows Services	Wählt die Ansicht "Management Windows Services" aus.

(siehe 96)	
MIB-Browser *(siehe 97)*	Wählt die Ansicht "MIB-Browser" aus.
Datensatzmanagerprotokoll *(siehe 100)*	Wählt das Datensatzmanagerprotokoll aus.
Syslog-Meldung *(siehe 101)*	Wählt die Ansicht "Syslog-Meldungen" aus.
Systemadministratorkonsole *(siehe 102)*	Wählt die Ansicht "Systemadministratorkonsole" aus.
Systemprotokoll *(siehe 104)*	Zeigt vom `Kaseya Network Monitor` Service erstellte Protokolleinträge an.
Trap-Meldungen *(siehe 104)*	Wählt die Ansicht "SNMP-Trap-Meldung" aus.
Eigene Einstellungen *(siehe 104)*	Wählt die Ansicht "Eigene Einstellungen bearbeiten" aus.
Benutzerbenachrichtigungsgruppen *(siehe 105)*	Verwaltet Benutzergruppen. Bestandsbenachrichtigungen werden an alle Mitglieder der Benutzergruppe gesendet, die mit diesem Bestand verknüpft sind.
Angepasste Datentypen *(siehe 106)*	Erstellt benutzerdefinierte Datentypen zur Verwendung bei Monitoren, die generische Daten speichern können.
Bestandsvorlagen *(siehe 107)*	Konfiguriert Monitorsets, die einem Bestand in einem Schritt zugewiesen werden können.
Protokolleinstellungen *(siehe 108)*	Legt Protokollrichtlinien für Network Monitor fest.
NOC-Konfiguration *(siehe 109)*	Erstellt benutzerdefinierte NOC-Ansichten (Network Operations Center, Netzwerkbetriebsansichten).
Weitere Systemeinstellungen *(siehe 109)*	Legt weitere Einstellungen für Benachrichtigungen und andere Ereignisse fest.
SMS *(siehe 110)*	Legt SMS-Nachrichteneinstellungen fest.

Berichte angepasst

Network Monitor > Berichte > Ansicht

Die Seite **Berichte angepasst** enthält alle angepassten Berichte. **Angepasste Berichte** sind für das Bestimmen von Berichten geeignet, deren Inhalt sich nicht ändert. Ein angepasster Bericht ist auch die einzige Möglichkeit, einen Bericht zu erstellen, der Daten für unterschiedliche Zeitperioden im gleichen Bericht erhält. Angepasste Berichte sind wie Berichtsvorlagen aufgebaut, *aber an spezifische Untergruppen, Bestände und Monitore gebunden.* Aus diesem Grund werden angepasste Berichte nicht ausgeführt, indem ein Knoten im Monitorbaum zuerst ausgewählt wird. *Stattdessen erstellen Sie angepasste Berichte und führen diese aus, indem Sie Network Monitor > Berichte > Ansicht auswählen.*

Die folgenden Unterthemen beschreiben **Berichtsvorlagen** *(siehe 80)* und angepasste Berichte. Bestimmte Felder gelten nur für angepasste Berichte und werden in jedem Thema identifiziert.

- **Berichtseigenschaften** *(siehe 81)*
- **Stilvorlagen** *(siehe 81)*
- **Berichtsdaten** *(siehe 82)*
- **Berichtsdatentypen** *(siehe 82)*
- **Diagramme** *(siehe 84)*
- **Datentabellen** *(siehe 85)*
- **Ausfallzeitbericht** *(siehe 86)*
- **Kommentare** *(siehe 87)*

- **Abbilder** *(siehe 87)*
- **Toplists** *(siehe 88)*

Aktionen

- **Löschen** – Löscht den ausgewählten Bericht.
- **Neuer angepasster Bericht (oder** **zum Bearbeiten)** – Bearbeitet die **Eigenschaften** *(siehe 81)* des Berichts.
- **(Angaben bearbeiten)** – Klicken Sie auf den **unterstrichenen Namen des Berichts** *(siehe 82)*, um die Liste der Designelemente im Bericht hinzuzufügen oder zu ergänzen.
- **(Bericht anzeigen)** – – Zeigt den ausgewählten angepassten Bericht in einem Browser an.
- **(E-Mail oder Veröffentlichen)** – – **Verteilt den Bericht** *(siehe 73)* als einen E-Mail-Anhang oder speichert den Bericht an einem Netzwerkspeicherort.

Berichtsvorlagen

Network Monitor > Berichte >Berichtsvorlagen

Die Seite **Berichtsvorlagen** enthält alle Berichtsvorlagen. Eine Berichtsvorlage hat ein vordefiniertes Layout, einen Satz an Datenobjekten und Designelemente. Berichtsvorlagen sind global und können überall angewendet werden. Sie können einen beliebigen Knoten auswählen und auf den Befehl **Einen Bericht erstellen > Im Browser anzeigen** klicken, um einen Bericht aus einer ausgewählten Berichtsvorlage zu generieren. Standardmäßig enthält der Bericht alle Bestände und Monitore, die im ausgewählten Knoten enthalten sind. Sie können dies auch direkt über die Seite **Berichtsvorlagen** ausführen.

Viele vordefinierte Berichtsvorlagen sind im **Network Monitor** enthalten. Sie können diese anpassen oder eigene erstellen.

Die folgenden Unterthemen beschreiben Berichtsvorlagen und **angepasste Berichte** *(siehe 79)*. Bestimmte Felder gelten nur für angepasste Berichte und werden in jedem Thema identifiziert.

- **Berichtseigenschaften** *(siehe 81)*
- **Stilvorlagen** *(siehe 81)*
- **Berichtsdaten** *(siehe 82)*
- **Berichtsdatentypen** *(siehe 82)*
- **Diagramme** *(siehe 84)*
- **Datentabellen** *(siehe 85)*
- **Ausfallzeitbericht** *(siehe 86)*
- **Kommentare** *(siehe 87)*
- **Abbilder** *(siehe 87)*
- **Toplists** *(siehe 88)*

Aktionen

- **Löschen** – Löscht den ausgewählten Bericht.
- **Neue Berichtsvorlage (oder** **zum Bearbeiten)** – Bearbeitet die **Eigenschaften** *(siehe 81)* des Berichts.
- **(Bericht konfigurieren)** – Klicken Sie auf den **unterstrichenen Namen des Berichts** *(siehe 82)*, um die Liste der Designelemente im Bericht zu konfigurieren.
- **(Bericht anzeigen)** – **– Zeigt die ausgewählte Berichtsvorlage in einem Browser an** *(siehe 70)*.
- **(E-Mail oder Veröffentlichen)** – – **Verteilt den Bericht** *(siehe 73)* als einen E-Mail-Anhang oder speichert den Bericht an einem Netzwerkspeicherort.

Berichtseigenschaften

Network Monitor > Berichte > Berichtsvorlagen > (klicken Sie auf das Symbol in einer Berichtsvorlage)
Network Monitor Berichte > Ansicht > (klicken Sie auf das Symbol in einem angepassten Bericht)

Die Seite **Berichtseigenschaften** legt die Basiseigenschaften der Berichtsvorlage oder des angepassten Berichts fest.

- **Name** – Geben Sie einen Namen für den Bericht ein. Der Name identifiziert den Bericht in der Listenansicht.
- **Description** – Eine längere Beschreibung des Berichts und seiner Funktion.
- **Berichtskategorie** – Wählen Sie die Kategorie für den Bericht aus. In der gesamten Benutzeroberfläche werden die Berichte nach Kategorie gruppiert.
- **Stil** – Wählen Sie die **Stilvorlage** *(siehe 81)* für den Bericht aus.
- **Favorit** – Wenn markiert, wird dieses Element für den aktuellen Benutzer als Favorit gekennzeichnet. Die favorisierten Elemente des aktuellen Benutzers kann auf einem Dashboard mithilfe des Favoriten-Widgets angezeigt werden.
- **Sichtbarkeit** – *Gilt nur für angepasste Berichte.*
  - **Privat** – Wenn diese Einstellung ausgewählt ist, kann nur der aktuelle Benutzer den angepassten Bericht in der Listenansicht sehen.
  - **Systemadministratoren** – Wenn diese Einstellung ausgewählt ist, können nur Sie und Systemadministratoren den angepassten Bericht in der Listenansicht sehen.

Berichtstile

Network Monitor > Berichte > Berichtstile

Stilvorlagen regeln das generelle Layout des Berichts. Eine Stilvorlage besteht aus einer Anzahl von verschiedenen Elementen, die für alle Berichte einheitlich sind, die dieselbe Stilvorlage verwenden. **Berichtsvorlagen** *(siehe 80)* und **Berichte angepasst** *(siehe 79)* können eine Stilvorlage verwenden.

Aktionen

- **Löschen** – Löscht die ausgewählte Stilvorlage.
- **Neue Stilvorlage (oder zum Bearbeiten)** – Fügt eine Stilvorlage hinzu oder bearbeitet diese. Die Registerkarte **Farbeinstellungen** wird nur im Bearbeitungsmodus angezeigt.

Basiseigenschaften

- **Name** – Dies ist der Name der Vorlage. Der Name wird verwendet, um die Vorlage in Listen zu identifizieren.
- **Beschreibung** – Eine längere Beschreibung der Stilvorlage.
- **Kopfzeile** – Die Kopfzeile wird am Seitenanfang aller generierten Berichte angezeigt. Der folgende Parameter kann in die Kopfzeile eingeschlossen werden.
  - `%[system.time]` – die aktuelle Zeit
- **Fußzeile** – Die Fußzeile wird am Seitenende eines jeden generierten Berichts angezeigt. Der folgende Parameter kann in die Fußzeile eingeschlossen werden.
  - `%[system.time]` – die aktuelle Zeit
- **Logo** – Es ist möglich, mithilfe dieser Vorlage jedem generierten Bericht ein Abbild hinzuzufügen, z. B. ein Logo. Logo-Abbilder müssen im Ordner `KNM\reports\images\logo` des KNM-Hostrechners gespeichert werden.
- **Logo-Platzierung** – Gibt die Platzierung eines Logo-Abbilds an.

- **Standard** – Markieren Sie diese Option, um diese Stilvorlage als Standard für neue Berichte festzulegen.

Farbeinstellungen

Legt alle Farben mithilfe des hexadezimalen `RRGGBB`-Farbformats fest.

- **Farbschema** – Wählen Sie ein vordefiniertes Farbschema. Zum Anpassen des eigenen Farbschemas wählen Sie `Custom`.
- **Hintergrund 1 und 2** – Geben Sie die Farbe für Hintergründe in Diagrammen ein.
- **Rasterfarbe** – Geben Sie die Farbe für das Raster in Diagrammen ein.
- **Textfarbe** – Geben Sie die Farbe für Text und Werte in Diagrammen ein.
- **Linienfarbe 1 bis 8** – Geben Sie die Farbe für jeden spezifischen Monitor in Diagrammen ein.

Berichtsdaten

Network Monitor > Berichte > Berichtsvorlagen > (klicken Sie auf den Namen der Berichtsvorlage)
Network Monitor > Berichte > Ansicht > (klicken Sie auf den Namen des angepassten Berichts)

Die Seite **Berichtsdaten** legt die Einzelheiten der Berichtsvorlage oder des angepassten Berichts fest. Dazu gehören das Layout, Designelemente und verwendete **Berichtsdatentypen** *(siehe 82)*.

Befehle

- **Bearbeiten** – (Sie können auch auf das Symbol klicken) – Bearbeitet das ausgewählte Element.
- **Kopieren** – Kopiert ein ausgewähltes Element.
- **Löschen** – Löscht ausgewählte Elemente.
- **Verfügbarkeit hinzufügen** – Fügt ein **Verfügbarkeitselement** *(siehe 86)* hinzu.
- **Kommentar hinzufügen** – Fügt ein **Kommentarelement** *(siehe 87)* hinzu.
- **Datentabelle hinzufügen** – Fügt ein **Datentabellenelement** *(siehe 85)* hinzu.
- **Grafik hinzufügen** – Fügt ein **Grafikelement** *(siehe 84)* hinzu. Klicken Sie auf den Hyperlink in einem Grafikelement, um die in dieser Grafik enthaltenen Monitore festzulegen.
- **Bild hinzufügen** – Fügt ein **Bildelement** *(siehe 87)* hinzu.
- **Maximumliste hinzufügen** – Fügt ein **Maximallistenelement** *(siehe 88)* hinzu.
- **(oder)** – Bewegt ein Element in der Liste nach oben oder unten.

Berichtsdatentypen

Die folgenden Typen an Datentypen können ausgewählt werden, wenn eine Grafik oder eine Datentabelle in einem Bericht festgelegt wird.

- Verfügbarkeit
  - Ausfallzeit Bericht für Bestände
  - Ausfallzeit Bericht für Monitore
- Datenbanken
  - Puffer-Cache-Trefferverhältnis
  - SQL-Anfragewert
- Umgebungsbedingungen
  - Temperatur

Luftfeuchtigkeit
Nässe
Spannung
Elektrischer Strom
Lüfterdrehzahl
Helligkeit
Relativer Luftstrom
Schalter/Trockenkontakt
Elektrische Energie

- Dateisystem
  - Plattenauslastung
  - Freier Festplattenspeicher
  - Verzeichnisgröße
  - Anzahl Verzeichnisdateien
  - Swap-Auslastung
- Netzwerk
  - Bandbreitenauslastung
  - Bandbreitennutzung
  - Ping-Roundtrip-Zeit
  - Ping-Paketverlust
  - Übertragungsgeschwindigkeit
  - Nicht festgelegte SNMP-Daten
  - Nicht festgelegte SSH-Skriptdaten
  - Verbindungen
  - Anforderungen
  - Anforderungen / Sek
  - Verbindungen / Sek
  - Benutzer
- Andere
  - Nicht festgelegte LUA-Daten
  - Latenz
- Leistung
  - CPU-Nutzung
  - Plattenauslastung
  - Freier Festplattenspeicher
  - Speicherauslastung
  - Freier Speicher
  - Swap-Auslastung
  - Nicht festgelegte Leistungsdaten Windows
  - Nicht festgelegte WMI-Daten
  - Nicht festgelegte Vmware-Leistungsdaten
  - Nicht festgelegte CIM-Leistungsdaten
- Benutzerdefiniert
  - (keine)
- Internet und E-Mail
  - E-Mail-Roundtrip-Zeit
  - Webseiten-Abrufzeit

Diagramme

Network Monitor > Berichte > Berichtsvorlagen > (klicken Sie auf den Namen einer Berichtsvorlage) > Fügen Sie ein Diagramm hinzu oder klicken Sie auf das Symbol eines Diagrammelements.
Network Monitor > Berichte > Ansicht > (klicken Sie auf den Namen eines angepassten Berichts) > Fügen Sie ein Diagramm hinzu oder klicken Sie auf das Symbol eines Diagrammelements.

Diagramme zeigen eine Grafik über einen bestimmten Zeitraum aufgezeichneter Monitordaten an. Jedes Diagramm kann Daten von bis zu acht einzelnen Monitoren beinhalten. Jeder Monitor ist mit einer bestimmten Farbe codiert. Die Farbe ist in der entsprechenden **Stilvorlage** *(siehe 81)* festgelegt.

Basiseigenschaften

- **Dauer** – Legt die Dauer dieses Elements fest. *Gilt nur für angepasste Berichte.*
  - `Current day`, `week`, `month`, `quarter`, `year`
  - `Last day`, `week`, `month`, `quarter`, `year`
  - `User defined period`
  - `Offset in days`

> **Hinweis:** Berichtsvorlagen legen die Zeitspanne fest, wenn die Berichtsvorlage ausgeführt wird.

- **Datentyp** – Wählt den **Datentyp** *(siehe 82)* und die Maßeinheit aus, um diese dem Bericht hinzuzufügen.
- **Kopfzeile** – Legt den Kopfzeilentext des Diagramms fest. Optional kann der folgende Parameter in die Kopfzeile miteinbezogen werden.
  - `%graph_type` – Zeigt den Berichtsdatentyp im Diagramm an.
- **Fußzeile** – Legt den Fußzeilentext des Diagramms fest.

Erweiterte Eigenschaften

- **Datenoption** – `average` (Standard), `min`, `max` – Definiert die Darstellungsart der Daten, wenn es mehrere Datensatzaufzeichnungen für einen bestimmten Zeitpunkt gibt. Betrifft nur die visuelle Darstellung.
- **Monitore trennen** – Bei Markierung wird jeder Monitor einzeln grafisch dargestellt.
- **Ausfüllen** – Bei Markierung wird das Diagramm ausgefüllt. Ignorieren Sie diese Option, wenn mehr als ein Monitor im Diagramm enthalten ist.
- **Beschriftung** – Bei Markierung wird eine Legende nach dem Diagramm eingefügt. Informationen zu allen in diesem Diagramm enthaltenen Monitoren sowie in diesem Zeitraum aufgetretene Extremwerte sind hier enthalten.
- **Datenfilter** – Legen Sie optional **Min** und **Max** für sichtbare Daten fest. Daten außerhalb dieses Bereichs werden ignoriert.
- **Benutzerdefinierter Maßstab** – Optional können Sie das Diagramm auf einen bestimmten Bereich der y-Achse beschränken. Dies wird normalerweise automatisch über den Datentyp gesteuert.
- **Diagrammgröße** – Legen Sie die Größe des Diagrammbilds fest. Der Standardwert ist 1000 x 152 Pixel.

Felder zur Berichtsanpassung (ausschließlich)

Zum **Berichte anpassen** klicken Sie auf den *Hyperlink* eines Diagrammelements, um die Seite **Monitor-Liste** anzuzeigen. Legen Sie fest, welche Monitore diesem Diagramm eingefügt werden.

- **Monitor hinzufügen** – Zeigt eine Seite **Monitore einem Diagramm hinzufügen** an.
  - **Monitor auswählen/Ausgewählte Monitore** – Geben Sie Text ein um die Namen der Monitore in der Liste **Monitor auswählen** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen

Sie ein oder mehrere Monitore in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um die Monitore der Liste **Ausgewählte Gruppen** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielmonitoren zu suchen. Um einen Monitor zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.

  - Es können Monitore ausgewählt werden, die Daten des im Diagramm festgelegten Typs speichern.

- **Löschen** – Löscht einen ausgewählten Monitor.
- (**oder**) – Bewegt ein Element in der Liste nach oben oder unten.

Datentabellen

Network Monitor > Berichte > Berichtsvorlagen > (klicken Sie auf den Namen einer Berichtsvorlage) > Fügen Sie eine Datentabelle hinzu oder klicken Sie auf das Symbol eines Datentabellenelements.
Network Monitor > Berichte > Ansicht > (klicken Sie auf den Namen eines angepassten Berichts) > Fügen Sie eine Datentabelle hinzu oder klicken Sie auf das Symbol eines Datentabellenelements.

Datentabellen können tabellarische Daten sowohl in horizontalen als auch vertikalen Tabellen anzeigen. Dadurch können Lesungen in einem Textformat angezeigt werden. Die Anzahl der Zeilen und Spalten hängt von der Berichtszeitdauer ab.

Datentabelleneigenschaften

- **Kopfzeile** – Kopfzeilentext, der Element im Bericht beschreibt.
- **Bestand auswählen/Ausgewählte Bestände** – Geben Sie Text ein, um die Namen der Bestände in der Liste **Bestand auswählen** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie einen Bestand oder mehrere Bestände in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um den Bestand der Liste **Ausgewählte Bestände** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielbeständen zu suchen. Um einen Bestand zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**. *Gilt nur für angepasste Berichte.*
- **Monitor auswählen/Ausgewählte Monitore** – Geben Sie Text ein um die Namen der Monitore in der Liste **Monitor auswählen** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie ein oder mehrere Monitore in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um die Monitore der Liste **Ausgewählte Gruppen** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielmonitoren zu suchen. Um einen Monitor zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**. *Gilt nur für angepasste Berichte.*
- **Dauer** – Legt die Dauer dieses Elements fest. *Gilt nur für angepasste Berichte.*
  - `Current day`, `week`, `month`, `quarter`, `year`
  - `Last day`, `week`, `month`, `quarter`, `year`
  - `User defined period`
  - `Offset in days`

  Hinweis: Berichtsvorlagen legen die Zeitspanne fest, wenn die Berichtsvorlage ausgeführt wird.

- **Lösung** – Die Frequenz innerhalb der **Dauer**, um Daten zu sammeln. *Gilt nur für angepasste Berichte.*
- **Layout** – Wählen Sie zwischen einem horizontalen Layout, in dem der zeitliche Verlauf von links nach rechts dargestellt wird und einem vertikalen Layout, wo der zeitliche Verlauf von oben nach unten gehend dargestellt wird.

Datentabellenkonfigurationen

Eine einzelne Datentabelle in einem Bericht umfasst eine oder mehrere Datentabellenkonfigurationen. Nach Auswahl eines **Datentyps** und des **Datentabellenmodus** klicken Sie auf die Schaltfläche **Hinzufügen**, um die Konfiguration zur Liste der Konfigurationen hinzuzufügen. Um eine Konfiguration zu entfernen, wählen Sie sie aus der Liste aus und klicken Sie auf die Schaltfläche **Entfernen**.

- **Datentyp** – Wählt **Datentyp** *(siehe 82)* und Maßeinheit, um sie dem Bericht hinzuzufügen.
- **Modus Datentabelle**
  - `Snapshot` – Die nächste Datenaufzeichnung für die Zelle. Beispiel: Wenn Sie einen `Daily` Bericht haben und es gibt zwei Aufzeichnungen um `14:59` und `15:02`, sind die angezeigten Daten für die Zelle um `15:00` die Aufzeichnung von `14:59`.
  - `Interval average` – Mittelt alle Aufzeichnungen innerhalb aller Zeiträume und verwendet diesen Wert für die entsprechende Zelle.
  - `Min` – Kleinste Datenaufzeichnung in jedem Zeitabschnitt.
  - `Max` – Größte Datenaufzeichnung in jedem Zeitabschnitt.

Ausfallzeitbericht

Network Monitor > Berichte > Berichtsvorlagen > (klicken Sie auf den Namen einer Berichtsvorlage) >
Network Monitor > Berichte > Ansicht > (klicken Sie auf den Namen eines angepassten Berichts > (klicken Sie auf das Symbol für eine Position)

Ausfallzeitbericht-Positionen (auch als *Verfügbarkeit* benannt) können die Ausfallzeit eines oder mehrerer ausgewählter Bestände oder individueller Monitore anzeigen. Ein Ausfallzeitbericht kann auch nach Tageszeit und Monitortyp gefiltert werden. Beispiel: Sie können die Ausfallzeit nur mithilfe von `Ping`-Monitoren berechnen.

Eigenschaften von Ausfallzeitberichten

Alle werden als Prozentzahlen des Berichtszeitraums berichtet.

- **Gruppe/Ausgewählte Gruppen** – Geben Sie Text ein um die Gruppennamen in der Liste **Gruppe** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie eine oder mehrere Gruppen in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um die Gruppen der Liste **Ausgewählte Gruppen** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielgruppen zu suchen. Um eine Gruppe zu entfernen, wählen Sie diese aus und klicken Sie auf die Schaltfläche **Entfernen**. *Gilt nur für angepasste Berichte.*
- **Dauer** – Legt die Dauer dieses Elements fest. *Gilt nur für angepasste Berichte.*
  - `Current day`, `week`, `month`, `quarter`, `year`
  - `Last day`, `week`, `month`, `quarter`, `year`
  - `User defined period`
  - `Offset in days`

  Hinweis: Berichtsvorlagen legen die Zeitspanne fest, wenn die Berichtsvorlage ausgeführt wird.

- **Reporting Ausfallzeit**
  - `Report downtime for assets` – Zeigt individuelle Bestände und deren Beitrag zur Ausfallzeit an.
  - `Report downtime for monitors` – Zeigt jeden Monitor in jedem Bestand und seinen Beitrag zur Ausfallzeit an.
- **Bericht Betriebszeit** – Die Zeit, in der sich der Monitor in einem normalen Status befunden hat.
- **Bericht Ausfallzeit** – Die Gesamtzeit, in der sich der Monitor in Alarmstatus befunden hat.

- **Bericht Unbekannte Zeit** – Unbekannt ist der Zeitraum, in dem **Network Monitor** den Monitorstatus nicht erkennt, z. B. wenn der **Network Monitor**-Service für einige Stunden angehalten wurde. Wenn nichts angegeben ist:
  - `Consider unknown time as uptime`
  - `Leave unknown time as unknown time`
- **Beinhaltet Bestände und Monitore ohne Ausfallzeit im Bericht** – Wenn nichts angegeben wird, werden Bestände aus dem Bericht entfernt, die keine Ausfallzeit-Probleme aufweisen.

Erweiterte Eigenschaften

- **Berechnung Ausfallzeit**
  - **SUM** – Addiert die Ausfallzeitwerte in dem Bericht.
  - **Durchschn.** – Liefert Durchschnitts-Ausfallzeit-Werte in dem Bericht an.
- **Zeitlimit** – Begrenzt die Ausfallzeit-Daten auf einen täglichen Stundenbereich.
- **Monitorlimit** – Begrenzt die Ausfallzeit-Daten auf angegebene **Monitortypen** *(siehe 115)*.

Kommentare

Network Monitor > Berichte > Berichtsvorlagen > (klicken Sie auf den Namen einer Berichtsvorlage) > Fügen Sie einen Kommentar hinzu oder klicken Sie auf das Symbol für eine Kommentar-Position.
Network Monitor > Berichte > Ansicht > (klicken Sie auf den Namen eines angepassten Berichts > Fügen Sie einen Kommentar hinzu oder klicken Sie auf das Symbol für eine Kommentar-Position.

Kommentare können Ihren Berichten hinzugefügt werden. Sie können auch verwendet werden, um Unterschriftenfelder für Situationen hinzuzufügen, in denen ein Bericht von einer anderen Person geprüft und unterschrieben werden muss.

- **Kommentar** – Der Kommentartext, der dem Bericht hinzugefügt wird.
- **Schriftartoptionen** – Die Schriftgröße und Ausrichtung des Kommentartexts.
- **Unterschriftenfeld** – Bei Markierung wird eine horizontale Linie im Bericht angezeigt, in dem eine Unterschrift eingefügt werden kann.

Abbilder

Network Monitor > Berichte > Berichtsvorlagen > (klicken Sie auf den Namen einer Berichtsvorlage) > Fügen Sie ein Bild hinzu oder klicken Sie auf das Symbol für eine Abbild-Position.
Network Monitor > Berichte > Ansicht > (klicken Sie auf den Namen eines angepassten Berichts > Fügen Sie ein Bild hinzu oder klicken Sie auf das Symbol für eine Abbild-Position.

Die Seite **Bericht Bild** fügt Kunden-Abbilder zu Ihren Berichten hinzu. Unterstützte Bilddateien müssen im Ordner `KNM\reports\images` des KNM-Hostrechners gespeichert werden. Dann ist es möglich, sie aus dieser Seite auszuwählen und in Berichten anzuzeigen.

- **Abbild** – Wählen Sie das gewünschte Abbild aus der Liste aus.
- **Platzierung** – Gibt die Platzierung eines Abbilds im Bericht an.

Toplists

Network Monitor > Berichte > Berichtsvorlagen > (klicken Sie auf den Namen einer Berichtsvorlage) > Fügen Sie eine Maximalliste hinzu oder klicken Sie auf das Symbol für eine Maximallisten-Position.
Network Monitor > Berichte > Ansicht > (klicken Sie auf den Namen eines angepassten Berichts) > Fügen Sie eine Toplist hinzu oder klicken Sie auf das Symbol für eine Toplist-Position.

Die **Toplists**-Berichtsposition fügt ein oder mehrere **Toplists** *(siehe 34)* in Ihre Berichte ein.

Toplist-Konfigurationen

Eine einzelne Toplist-Position in einem Bericht umfasst eine oder mehrere Toplist-Konfigurationen. Nach Auswahl von **Typ, Sortiermodus, Einträge** und der **Daten**werte klicken Sie auf die Schaltfläche **Hinzufügen**, um die Konfiguration zur Liste der Konfigurationen hinzuzufügen. Um eine Konfiguration zu entfernen, wählen Sie sie aus der Liste aus und klicken Sie auf die Schaltfläche **Entfernen**.

- **Kopfzeile** – Kopfzeilentext, der die Position im Bericht beschreibt.
- **Dauer** – Wählt die Toplist aus, die dem Bericht hinzugefügt wird.
  - `Current day`
  - `Current week`
  - `Current month`
  - `Last day`
  - `Last week`
  - `Last month`
- **Typ** – Wählt den Datentyp aus.
  - `Bandwidth usage`
  - `Bandwidth utlization`
  - `CPU utilization`
  - `Disk utilization`
  - `Fan speed`
  - `Free disk space`
  - `Free memory`
  - `Humidity`
  - `Luminosity`
  - `Memory utilization`
  - `Ping packetloss`
  - `Ping roundtrip time`
  - `Relative airflow`
  - `Swap utilization`
  - `Temperature`
  - `Transfer speed`
  - `Webpage fetch time`
  - `Wetness`
- **Sortiermodus**
  - `Lowest entries first`
  - `Highest entries first`
- **Einträge** – Anzahl der angezeigten Einträge.

- **Daten**
  - `Sampled min value`
  - `Sampled max value`
  - `Period average`
- **Hinzufügen / Ausgewählt / Entfernen** – Zum Hinzufügen einer Toplist-Konfiguration klicken Sie auf die Schaltfläche **Hinzufügen**. Die ausgewählte Konfiguration wird zur Liste **Ausgewählt** hinzugefügt. Um eine Konfiguration zu entfernen, wählen Sie sie aus und klicken Sie auf die Schaltfläche **Entfernen**.

Nur Felder für Berichtsvorlagen

- **Filtern nach Auswahl** – Bei Markierung werden Bestände und Monitore ausgewählt, wenn die Berichtsvorlage im Bericht angezeigt wird. Diese Option ist standardmäßig ausgewählt.

Felder zur Berichtsanpassung (ausschließlich)

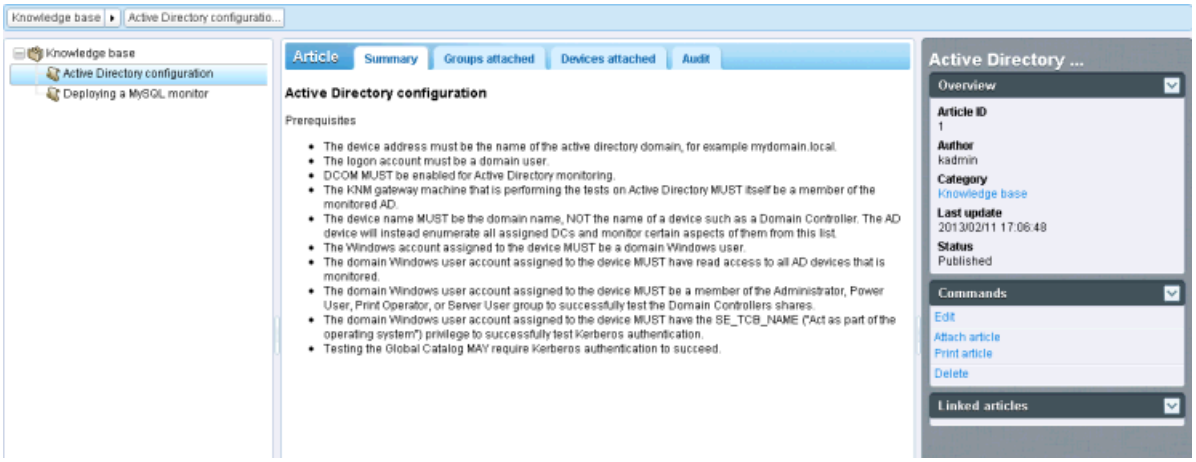
Die folgenden Felder werden nur für angepasste Berichte angezeigt.

- **Gruppe/Ausgewählte Gruppen** – Geben Sie Text ein um die Gruppennamen in der Liste **Gruppe** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie eine oder mehrere Gruppen in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um die Gruppen der Liste **Ausgewählte Gruppen** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielgruppen zu suchen. Um eine Gruppe zu entfernen, wählen Sie diese aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Bestand auswählen/Ausgewählte Bestände** – Geben Sie Text ein, um die Namen der Bestände in der Liste **Bestand auswählen** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie einen Bestand oder mehrere Bestände in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um den Bestand der Liste **Ausgewählte Bestände** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielbeständen zu suchen. Um einen Bestand zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.

Knowledge-Base-Artikel

Network Monitor > Knowledgebase > Ansicht

Mit **Knowledge-Base** können Sie einen freigegebenen Satz an Artikeln für Kurzanleitungen erstellen, der einer Gruppe, einem Bestand oder Monitor zugewiesen werden kann. Damit erhalten Sie sofortigen Zugriff auf das Referenzmaterial, das Sie für die Fehlersuche und zum Verwalten der Bestände benötigen. Klicken Sie auf eine Gruppe, ein Gateway oder einen Bestandsknoten und wählen Sie die Registerkarte **Knowledge-Base** *(siehe 37)* aus, um die Liste der **Knowledge-Base**-Artikel anzuzeigen, die diesem Knoten zugewiesen sind.


Knowledge base
Active Directory configuratio...
Knowledge base
Active Directory configuration
Deploying a MySQL monitor
Article
Summary
Groups attached
Devices attached
Audit
Active Directory configuration
Prerequisites
The device address must be the name of the active directory domain, for example mydomain.local.
The logon account must be a domain user.
DCOM MUST be enabled for Active Directory monitoring.
The KNM gateway machine that is performing the tests on Active Directory MUST itself be a member of the monitored AD.
The device name MUST be the domain name, NOT the name of a device such as a Domain Controller. The AD device will instead enumerate all assigned DCs and monitor certain aspects of them from this list.
The Windows account assigned to the device MUST be a domain Windows user.
The domain Windows user account assigned to the device MUST have read access to all AD devices that is monitored.
The domain Windows user account assigned to the device MUST be a member of the Administrator, Power User, Print Operator, or Server User group to successfully test the Domain Controllers shares.
The domain Windows user account assigned to the device MUST have the SE_TCB_NAME ("Act as part of the operating system") privilege to successfully test Kerberos authentication.
Testing the Global Catalog MAY require Kerberos authentication to succeed.
Active Directory ...
Overview
Article ID
1
Author
kadmin
Category
Knowledge base
Last update
2013/02/11 17:06:48
Status
Published
Commands
Edit
Attach article
Print article
Delete
Linked articles

Verwandte Themen

- **Registerkarte "Knowledge"** *(siehe 37)*
- **Knowledge-Base-Kategorien** *(siehe 91)*

Registerkarten anzeigen

- **Zusammenfassung** – Zeigt den Artikel an.
- **Registerkarte** Hinzugefügte Gruppen – Zeigt die Gruppen an, die dem aktuellen Artikel hinzugefügt wurden. Fügt optional den aktuellen Artikel Gruppen und Beständen hinzu oder entfernt diesen.
- **Registerkarte** Hinzugefügte Bestände – Zeigt die Bestände an, die dem aktuellen Artikel hinzugefügt wurden. Fügt optional den aktuellen Artikel Gruppen und Beständen hinzu oder entfernt diesen.
- **Registerkarte** Audit – Zeigt das Protokoll der Benutzer an, die den Artikel aktualisiert haben.

Befehle

- **Bearbeiten** – Bearbeitet den ausgewählten Artikel.
- **Artikel hinzufügen** – Fügt den aktuellen Artikel Gruppen und Beständen hinzu.
- **Artikel drucken** – Druckt den aktuellen Artikel.
- **Löschen** – Löscht den aktuellen Artikel.

Registerkarte bearbeiten

- **Registerkarte** Basiseigenschaften – Bearbeitet den Titel und Inhalt eines Artikels. Verwenden Sie die folgenden Schaltflächen in der Symbolleiste, um eine spezielle Formatierung dem Text hinzuzufügen:

Die erweiterten Schaltflächen der Symbolleiste sind nachfolgend beschrieben.

- – Quelle – Ermöglicht Ihnen, die HTML-Tags zu bearbeiten, die das Format des Artikels steuern
- – Zeigt die Wiedergabe von Text und Bildern in einer Vorschau an.
- – Setzt kopierten Inhalt aus einem Word-Dokument ein.
- – Suchen und ersetzen.
- – Formatierung entfernen.
- – Verknüpft Text mit einer URL, einem Anker oder einer Element-ID und hebt die Verknüpfung wieder auf. Links werden nur innerhalb desselben Artikels unterstützt.
  - ✓ Fügen Sie einen benannten Anker an einer Position im Artikeltext ein. Fügen Sie dann einen Link ein, durch den der Artikel zu dem benannten Anker springt, wenn Sie auf den Link klicken.
  - ✓ Verwenden Sie das Symbol Quelle, um HTML-Tags anzuzeigen und ein ID-Attribut einem Element hinzuzufügen. Fügen Sie dann einen Link ein, durch den der Artikel zu der Element-ID springt, wenn Sie auf den Link klicken.
- – Fügt eine Tabelle an der Position des Cursors ein. Zu den Tabelleneigenschaften gehören die Anzahl an Zeilen und Spalten, Überschrift, Rahmenbreite, Kopfzeile, Abstand zwischen den Zellen, Ausrichtung.
- – Horizontale Linie als einen Prozentsatz der Breite einfügen oder eine feste Breite in Pixel festlegen
- – Fügt ein Emoticon ein.
- – Fügt ein Symbol ein.
- – Fügt einen Seitenumbruch ein. Beim Drucken eines Artikels verwendet.

- **Registerkarte** erweitert
  - **Kategorien verknüpfen / Verknüpfte Kategorien** – Verknüpft explizit einen Artikel mit mindestens einer Kategorie. Eine Kategorie ist ein Knowledge-Base-Ordner, der andere Kategorien oder Knowledge-Base-Artikel enthält. Durch Klicken auf eine Kategorie werden alle Artikel aufgeführt, die mit dieser Kategorie verknüpft sind.
  - **Verwandte Artikel hinzufügen / Verwandte Artikel** – Verknüpft einen Artikel mit anderen verwandten Artikeln. Verwandte Artikel werden auf der rechten Seite des Felds aufgeführt, wenn ein Artikel angezeigt wird.

Weitere Informationen siehe auch:

- **Knowledge-Base-Kategorien** *(siehe 91)*
- **Registerkarte "Knowledge"** *(siehe 37)*

Knowledge-Base-Kategorien

Eine Knowledge-Base-**Kategorie** ist ein Knowledge-Base-Ordner, der andere Kategorien oder Knowledge-Base-Artikel enthält. Durch Klicken auf eine Kategorie im Knowledge-Base-Baum werden alle Artikel im mittleren Feld aufgelistet, die entweder Nachfolger dieser Kategorie oder mit dieser Kategorie *explizit verknüpft* sind. Artikel werden explizit mit Kategorien verknüpft, indem die Registerkarte Bearbeiten **Erweitert** *(siehe 89)* verwendet wird, um einen Artikel zu bearbeiten.

Verwandte Themen

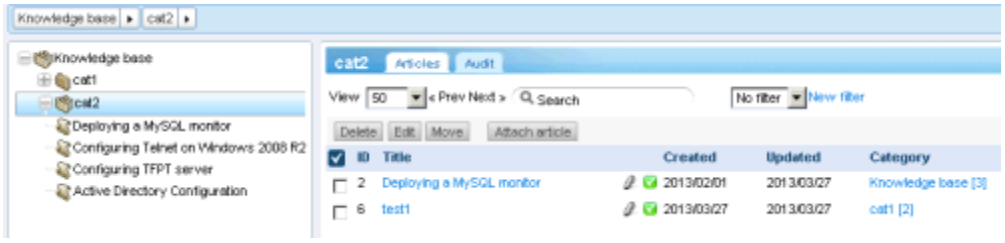
- **Knowledge-Base-Artikel** *(siehe 89)*
- **Registerkarte "Knowledge"** *(siehe 37)*

Aktionen

- **Löschen** – Löscht einen ausgewählten Artikel.
- **Bearbeiten** – Bearbeitet einen oder mehrere Artikel. Wenn mehrere Artikel bearbeitet werden, können nur geteilte Eigenschaften bearbeitet werden.
- **Verschieben** – Verschiebt ausgewählte Artikel an eine andere Position im Knowledge-Base-Baum. *Dies beeinflusst nicht explizite Verknüpfungen zwischen Artikeln und Kategorien.*
- **Artikel hinzufügen** – Fügt einen Artikel zu ausgewählten Gruppen und Beständen hinzu.

Befehle

- **Bearbeiten** – Bearbeitet einen ausgewählten Artikel.
- **Unterkategorie hinzufügen** – Fügt eine Unterkategorie der aktuellen Kategorie hinzu.
- **Kategorie löschen** – Löscht die aktuelle Kategorie.
- **Neuen Artikel erstellen** – Erstellt einen neuen Artikel, der der aktuellen Kategorie untergeordnet ist.



Registerkarte bearbeiten

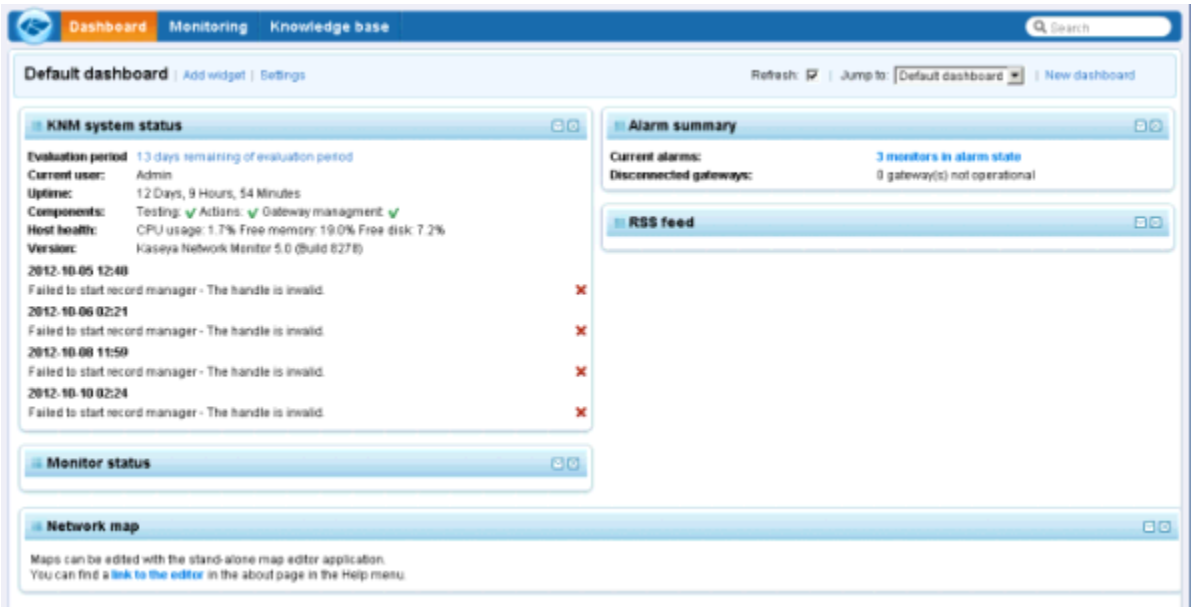
Registerkarte "Basiseigenschaften"

- **Name** – Der Name der Kategorie.
- **Beschreibung** – Eine Beschreibung der Kategorie in einer Zeile.

Dashboard

Network Monitor > Dashboard>-Ansicht

Das **Network Monitor**-Dashboard ist eine durch den Benutzer konfigurierbare Ansicht, die ein oder mehrere *Widgets* umfasst. Jedes Widget zeigt einen unterschiedlichen Typ an Echtzeitinformationen an.


Dashboard
Monitoring
Knowledge base
Default dashboard
Add widget | Settings
Refresh:
Jump to:
Default dashboard
New dashboard
KNM system status
Evaluation period 13 days remaining of evaluation period
Current user: Admin
Uptime: 12 Days, 9 Hours, 54 Minutes
Components: Testing: Actions: Gateway management:
Host health: CPU usage: 1.7% Free memory: 19.0% Free disk: 7.2%
Version: Kaseya Network Monitor 5.0 (Build 8278)
2012-10-05 12:48
Failed to start record manager - The handle is invalid.
2012-10-06 02:21
Failed to start record manager - The handle is invalid.
2012-10-08 11:59
Failed to start record manager - The handle is invalid.
2012-10-10 02:24
Failed to start record manager - The handle is invalid.
Alarm summary
Current alarms: 3 monitors in alarm state
Disconnected gateways: 0 gateway(s) not operational
RSS feed
Monitor status
Network map
Maps can be edited with the stand-alone map editor application.
You can find a link to the editor in the about page in the Help menu.

Eine Reihe von nützlichen Widgets sind im **Network Monitor** enthalten. Dazu gehören:

- Status-Widgets
  - Monitorstatus
  - Bestandsstatus
  - Untergruppenstatus
  - Gateway-Status
  - Benutzerstatus
  - Systemstatus
  - Alarmübersicht
  - NOC-Widget
- Karten-Widgets
  - Netzwerkkarte
  - Netzwerkkarte, klein
- Sonstige Widgets
  - Webseite
  - Webseite, klein
  - Favorisierte Elemente
  - Protokolleinträge
  - Toplists
  - Notepad
  - RSS-Feed

Klicken Sie auf **Einstellungen**, um ein Dashboard zu erstellen oder zu bearbeiten. Klicken Sie auf **Widget hinzufügen**, um Widgets einem Dashboard hinzuzufügen.

Bestandswartung

Network Monitor > Zeitpläne > Bestandswartung

Die Seite **Bestandswartung** plant Ausfallzeiten durch Wartungszeiten für *Bestände*. Während einer geplanten Wartungszeit werden keine Monitore überprüft. Wartungspläne können sich entweder auf eine einzige Wartungszeit oder eine wiederkehrende Wartungszeit mit vielen flexiblen Planungsoptionen beziehen.

Aktionen

UMSCHALTTASTE + Klicken, um mehrere Zeilen auszuwählen.

- **Löschen** – Löscht ausgewählte Zeitpläne.
- **(Bearbeiten)** – Klicken Sie auf das Symbol Eigenschaften, um eine einzelne Zeile zu bearbeiten.
- **Neue Planung** – Erstellt eine **neue Planung** *(siehe 93)*.

Bestandswartung bearbeiten

Network Monitor > Zeitpläne > Bestandswartung > Neue Planung oder Bearbeiten

Die Seite **Bestandswartung bearbeiten** legt einen einzelnen Wartungsplan fest, der auf *mehrere* Bestände angewendet werden kann. Der Plan kann für einen einzelnen Zeitraum oder wiederkehrende Zeiträume gelten.

> **Hinweis:** Einfache Wartung für einen *einzelnen* Bestand kann in der Registerkarte **Erweitert** *(siehe 50)* in einem Bestandsknoten festgelegt werden.

Wartungseinstellungen

- **Bestände auswählen** – Geben Sie eine Zeichenfolge in das Feld "Bearbeiten" ein, um alle Bestandsnamen anzuzeigen, die dem String entsprechen Klicken Sie dann auf die Schaltfläche **Hinzufügen**. Sie können auch die Schaltfläche **Markieren** verwenden, um nach den Beständen zu suchen.
- **Ausgewählte Bestände** – Zeigt ausgewählte Bestände an. Zum Entfernen von Elementen wählen Sie die Elemente in der Liste aus und klicken Sie dann auf **Entfernen**.
- **Startzeit** – Gibt die Uhrzeit an, zu der die Wartungszeit gestartet wird.
- **Wartungszeit** – Gibt die Dauer der Wartungszeit in Stunden und Minuten an.
- **Wartungsmodus** – `Stop tests during maintenance`. Dies ist der einzige Modus, der zurzeit unterstützt wird.
- **Läuft ab** – Bei Markierung wird der Wartungsplan nach Ablauf der Wartungszeit automatisch gelöscht.
- **Beschreibung** – Beschreibt den Wartungsplan.
- **Zeitplantyp**
  - **Einzelne Wartung**
    - ✓ **Startdatum** – Gibt das Datum an, an dem der Wartungsplan aktiviert wird. Geben Sie das Datum im Format `YYYY-MM-DD` an.
  - **Wiederholte Wartung**
    - ✓ **Aktiv zwischen** – Gibt den Datumsbereich an, in dem der Wartungsplan aktiv ist. Geben Sie den Datumsbereich im Format `YYYY-MM-DD` an. Werden diese Felder nicht ausgefüllt, ist der Wartungsplan immer aktiv.
    - ✓ **Wochentag** – Durch Festlegen eines Tages ist der Wartungsplan nur an den ausgewählten Tagen aktiv.
    - ✓ **Jeder x-te Tag** – Wenn dies aktiviert ist, ist der Wartungsplan an jedem x-ten Tag ab

angegebenem Startdatum aktiv. Für diese Option muss ein Datumsbereich in den Feldern **Aktiv zwischen** angegeben werden.

- ✓ **Letzter Tag im Monat** – Bei Markierung ist der Wartungsplan am letzten Tag jedes Monats aktiv.
- ✓ **Tage im Monat** – Bei Markierung ist der Wartungsplan an bestimmten Tagen im Monat aktiv. Geben Sie die Tage ein, getrennt durch ein Komma.

Monitorwartung

Network Monitor > Zeitpläne > Pflege überwachen

Die Seite **Pflege überwachen** plant Ausfallzeiten durch Wartungszeiten für *Monitore*. Während einer geplanten Wartungszeit werden keine Monitore überprüft. Wartungspläne können sich entweder auf eine einzige Wartungszeit oder eine wiederkehrende Wartungszeit mit vielen flexiblen Planungsoptionen beziehen.

Aktionen

UMSCHALTTASTE + Klicken, um mehrere Zeilen auszuwählen.

- **Löschen** – Löscht ausgewählte Zeitpläne.
- **(Bearbeiten)** – Klicken Sie auf das Symbol Eigenschaften, um eine einzelne Zeile zu bearbeiten.
- **Neue Planung** – Erstellt eine **neue Planung** *(siehe 94)*.

Pflege überwachen bearbeiten

Network Monitor > Zeitpläne > Pflege überwachen > Neue Planung oder Bearbeiten

Die Seite **Pflege überwachen bearbeiten** gibt einen Wartungsplan an, der auf *mehrere* Monitore angewendet werden kann. Der Plan kann für einen einzelnen Zeitraum oder wiederkehrende Zeiträume gelten.

Hinweis: Eine einfache Wartung für einen *einzelnen* Monitor kann in der Registerkarte **Erweitert** *(siehe 63)* in einem Monitor-Knoten festgelegt werden.

Wartungseinstellungen

- **Bestände auswählen** – Geben Sie eine Zeichenfolge in das Feld "Bearbeiten" ein, um alle Bestandsnamen anzuzeigen, die dem String entsprechen Klicken Sie dann auf die Schaltfläche **Hinzufügen**. Sie können auch die Schaltfläche **Markieren** verwenden, um nach den Beständen zu suchen.
- **Ausgewählte Bestände** – Zeigt ausgewählte Bestände an. Zum Hinzufügen von Elementen, wählen Sie die Elemente in der Liste aus und klicken Sie dann auf **Entfernen**.
- **Startzeit** – Gibt die Uhrzeit an, zu der die Wartungszeit gestartet wird.
- **Wartungszeit** – Gibt die Dauer der Wartungszeit in Stunden und Minuten an.
- **Wartungsmodus** - `Stop tests during maintenance`. Dies ist der einzige Modus, der zurzeit unterstützt wird.
- **Läuft ab** – Wenn diese Option markiert ist, wird der Wartungsplan nach Ablauf der Wartungszeit automatisch gelöscht.
- **Beschreibung** – Beschreibt den Wartungsplan.
- **Zeitplantyp**
  - ➢ **Einzelne Wartung**
    - ✓ **Startdatum** – Gibt das Datum an, an dem der Wartungsplan aktiviert werden soll.

Geben Sie das Datum im Format `YYYY-MM-DD` an.

- **Wiederholte Wartung**
  - ✓ **Aktiv zwischen** – Gibt den Datumsbereich an, in dem der Wartungsplan aktiv ist. Geben Sie den Datumsbereich im Format `YYYY-MM-DD` an. Werden diese Felder nicht ausgefüllt, ist der Wartungsplan immer aktiv.
  - ✓ **Wochentag** – Durch Festlegen eines Tages ist der Wartungsplan nur an den ausgewählten Tagen aktiv.
  - ✓ **Jeder x-te Tag** – Wenn festgelegt, ist der Wartungsplan an jedem x-ten Tag ab angegebenem Startdatum aktiv. Für diese Option muss ein Datumsbereich in den Feldern **Aktiv zwischen** angegeben werden.
  - ✓ **Letzter Tag im Monat** – Wenn festgelegt, ist der Wartungsplan am letzten Tag jedes Monats aktiv.
  - ✓ **Tage im Monat** – Wenn festgelegt, ist der Wartungsplan an bestimmten Tagen im Monat aktiv. Geben Sie die Tage ein, getrennt durch ein Komma.

Benutzerbenachrichtigungspläne

Network Monitor > Zeitpläne > Benutzerbenachrichtigungspläne

Die Seite **Benutzerarbeitspläne** plant *aktive* Zeiträume für *Benutzer*. Dadurch erhalten Operatoren keine Benachrichtigungen außerhalb ihrer Arbeitszeit.

Aktionen

UMSCHALTTASTE + Klicken, um mehrere Zeilen auszuwählen.

- **Löschen** – Löscht Arbeitspläne des ausgewählten Benutzers.
- **(Bearbeiten)** – Klicken Sie auf das Symbol Eigenschaften, um eine einzelne Zeile zu **bearbeiten** *(siehe 96)*.
- **Neue Planung** – Erstellt eine neue Planung.

Verwandte Themen

- **Benutzerarbeitsplan bearbeiten** *(siehe 95)*
- **Zeitplanblöcke** *(siehe 96)*

Benutzerarbeitsplan bearbeiten

Network Monitor > Zeitpläne > Benutzerbenachrichtigungspläne > Neuer Zeitplan oder Bearbeiten

Die Seite **Benutzerarbeitsplan bearbeiten** legt den Arbeitsplan für einen einzelnen Benutzer fest. Sie legen die aktiven Tage und Stunden sowie die Benutzer fest, die mit einem Zeitplan verknüpft sind. Verwenden Sie dazu die Seite **Zeitplanblöcke** *(siehe 96)*.

Eigenschaften Zeitplan

- **Name** – Der Name des Benutzerarbeitsplans.
- **Description** – Eine längere Beschreibung des Benutzerarbeitsplans.
- **Aktiv** – Das Start- und Enddatum, zu dem der Benutzerarbeitsplan aktiv ist.
- **Läuft ab** – Wenn festgelegt, wird der Zeitplan nach dem aktiven Enddatum vom **Network Monitor** gelöscht.

Zeitplanblöcke

Network Monitor > Zeitpläne > Benutzerbenachrichtigungspläne > Klicken Sie auf den <Namen des Zeitplans>

Benutzerarbeitspläne *(siehe 95)* werden mit *Blöcken* und *Regeln festgelegt.*

- **Blöcke** – Ein Benutzerarbeitsplan wird in ein oder mehrere Blöcke unterteilt. Ein Block stellt einen kürzeren Zeitraum innerhalb des Zeitplans dar. Fügen Sie Blöcke hinzu, um eine Sequenz aus Blöcken zu erstellen. Sie können die Blöcke in der Sequenz nach oben und unten verschieben. Die Sequenz aus Blöcken wird fortlaufend vom aktiven Startdatum bis zum aktiven Enddatum des Zeitplans als *Gleitender Zeitplan* wiederholt.
- **Regeln** – Die für eine Regel ausgewählten Benutzer sind während der Tage und Stunden, die in einer Regel festgelegt sind, "aktiv". Sie können während dieser aktiven Zeiträume Benachrichtigungen empfangen. Sie können für jeden Block einen oder mehrere Regeln festlegen. Regeln können einander überlappen und verschiedene Benutzer festlegen.

Beispiel

1. Erstellen Sie für einen Monat einen Benutzerarbeitsplan.
2. Erstellen Sie einen Block, der sieben Tage lang ist.
3. Erstellen Sie zwei Regeln für diesen einzelnen Block: einen Wochentagblock und einen Wochenendeblock. Stellen Sie entsprechend Tage, Stunden und Benutzer für jede Regel ein.

Befehle

- **Bearbeiten** – Bearbeitet den Namen, das Start- und Enddatum des **Benutzerarbeitsplans** *(siehe 95)*.
- **Kopie** – Erstellt einen neuen Zeitplan, indem der aktuell ausgewählte Zeitplan kopiert wird.
- **Löschen** – Löscht den aktuell ausgewählten Zeitplan.

Blockaktionen

- **Block hinzufügen** (oder zum Bearbeiten) – Fügt einen Block hinzu oder bearbeitet diesen.
  - **Länge** – Geben Sie die Länge des Blocks in Tagen ein. Wenn Sie zum Beispiel sieben eingeben, wird ein Block mit der Länge von sieben Tagen erstellt.
- **Löschen** – Löscht ausgewählte Blöcke.

Regelaktionen

- **Regel bearbeiten** – Klicken Sie hier, um folgende Optionen zu bearbeiten.
  - **Wochentag** – Die Tage der Woche, an denen diese Regel aktiv ist.
  - **Aktiv zwischen** – Start- und Endzeit an dem Tag, an dem diese Regel aktiv ist.
  - **Verfügbare Benutzer** – Benutzer, die ausgewählt werden können.
  - **Ausgewählte Benutzer** – Die ausgewählten Benutzer sind während der für die Regel festgelegten Tage und Stunden aktiv und können Benachrichtigungen erhalten.
- **Regel löschen** – Löscht ausgewählte Regeln.

Liste der Windows-Dienste

Network Monitor > Werkzeuge > Windows-Dienste verwalten

Die **Liste der Windows-Dienste** ermöglicht Ihnen den direkten Zugriff auf eine Liste aller verfügbaren Dienste auf einem Windows-Computer. Es können nur Bestände ausgewählt werden, die als Windows-Computer identifiziert wurden und mit **Windows-Anmeldekonten zur Authentifizierung** *(siehe 40)* ausgestattet sind.

Anzeigen einer Liste verfügbarer Windows-Dienste

Geben Sie Text in das Feld **Bestand auswählen** ein, um sich die Namen der Bestände anzeigen zu lassen, die mit dem eingegebenen Text übereinstimmen. Wählen Sie einen Bestand aus. Klicken Sie auf die Schaltfläche **Aktualisieren**, um den Bestand zu der unter **Bestand auswählen** angezeigten Liste hinzuzufügen. Sie können auch auf die Schaltfläche **Auswählen** klicken, um nach Zielgruppen zu suchen.

Aktionen

Wählen Sie einen oder mehrere Bestände aus der Liste aus und führen Sie dann eine der folgenden Aktionen aus:

- **Start** – Starten Sie die ausgewählten Dienste.
- **Stopp** – Beenden Sie die ausgewählten Dienste.
- **Neu starten** – Starten Sie die ausgewählten Dienste neu.
- **Anhalten** – Halten Sie die ausgewählten Dienste an. Nicht alle Dienste können angehalten werden.
- **Fortsetzen** – Setzen Sie die Ausführung angehaltener Dienste fort.

Weitere Informationen siehe auch:

- **Windows-Dienststeuerung** *(siehe 163)* (Aktion)
- **Windows-Dienststeuerung** *(siehe 172)* (geplantes Ereignis)
- **Windows-Dienststatus** *(siehe 152)* (Monitor)

MIB Browser

Network Monitor > Werkzeuge > MIB-Browser
(Bestandsname) > Befehl ''MIB-Browser öffnen''
(Bestandsname) > Neuen Monitor hinzufügen > SNMP > OID [...]
(Bestandsname) > Neuen Monitor hinzufügen > SNMP-Trap > Filter ''OID einschließen/ausschließen'' [...]

Auf der Seite **MIB-Browser** finden Sie eine MIB-Baumstruktur, durch die Sie navigieren können, um **OID-Werte** *(siehe 98)* auszuwählen. *Damit Sie in diesem Dialog OID-Werte abrufen und auswählen können, muss der* **MIB-Browser** *erfolgreich eine Verbindung zum SNMP-Agent auf dem Remote-Bestand bzw. -Computer herstellen können.*

Es stehen Ihnen fünf Filterfelder zur Verfügung, um OID-Werte und entsprechende Werte auf einem Remote-Bestand festzulegen. Konnte die Verbindung erfolgreich hergestellt werden und wird die ausgewählte OID vom Remote-Bestand unterstützt, so wird der OID-Wert in der rechten oberen Ecke angezeigt, sobald Sie eine OID-Position in der Baumstruktur anklicken.

- **Host-Name** – Der Name des Bestands.
- **Port** – Standardmäßig auf 161 eingestellt.
- **Gateway** – Das vom Bestand genutzte Gateway.
- **SNMP-Version** – Die Version des SNMP-Protokolls, die für die Verbindung zum SNMP-Agent auf dem Bestand verwendet wird: `v1`, `v2c`, `v3`
- **Community mit Lesezugriff** – Der Name der Community mit SNMP-Lesezugriff, der dem Bestand zugewiesen wurde, mit dem Sie sich verbinden. Wird angezeigt, wenn "v1" und "v2c" ausgewählt werden.

Hinweis: Wie Sie Änderungen an der in diesem Dialog angezeigten MIB-Baumstruktur vornehmen, erfahren Sie im Abschnitt **Kompilieren von benutzerdefinierten MIB-Dateien** *(siehe 99)*.

Auswählen einer OID

1. Wenn Sie eine OID in der Baumstruktur auf der linken Seite anklicken, werden die Eigenschaften dieser OID auf der rechten Bildschirmseite angezeigt.

Hinweis: OID-Werte werden nur dann zurückgegeben, wenn eine Verbindung zum Bestand besteht und der Bestand die ausgewählte OID-Anfrage unterstützt.

---

2. Klicken Sie auf die Schaltfläche **OID auswählen**.

MIB-Objekte

Jeder SNMP-aktivierte Bestand antwortet nur auf einen bestimmten Satz an SNMP-Anforderungen. Jede SNMP-Anforderung wird eindeutig durch eine Objekt-ID oder **OID** identifiziert. Beispiel: Eine OID mit der Bezeichnung `ifInOctets` wird durch zahlenbasierte OID `.1.3.6.1.2.1.2.2.1.10` wiedergegeben. Die entsprechende zeichenbasierte OID für `ifInOctets` ist `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets`.

Jeder Gerätehersteller veröffentlicht die OIDs, die von den SNMP-aktivierten Geräten des Herstellers unterstützt werden, und zwar in Form einer **MIB-Datei**. OIDs werden meistens als **MIB-Objekte** bezeichnet. Die MIB-Dateien können in eine "MIB-fähige" Anwendung importiert werden, z. B. **Network Monitor**. **Network Monitor** ist bereits mit vielen gängigen Sätzen an MIB-Objekten vorinstalliert. Damit ist das **Kompilieren von benutzerdefinierten MIB-Dateien** *(siehe 99)* normalerweise nur für Geräte mit speziellen MIB-Objekten erforderlich.

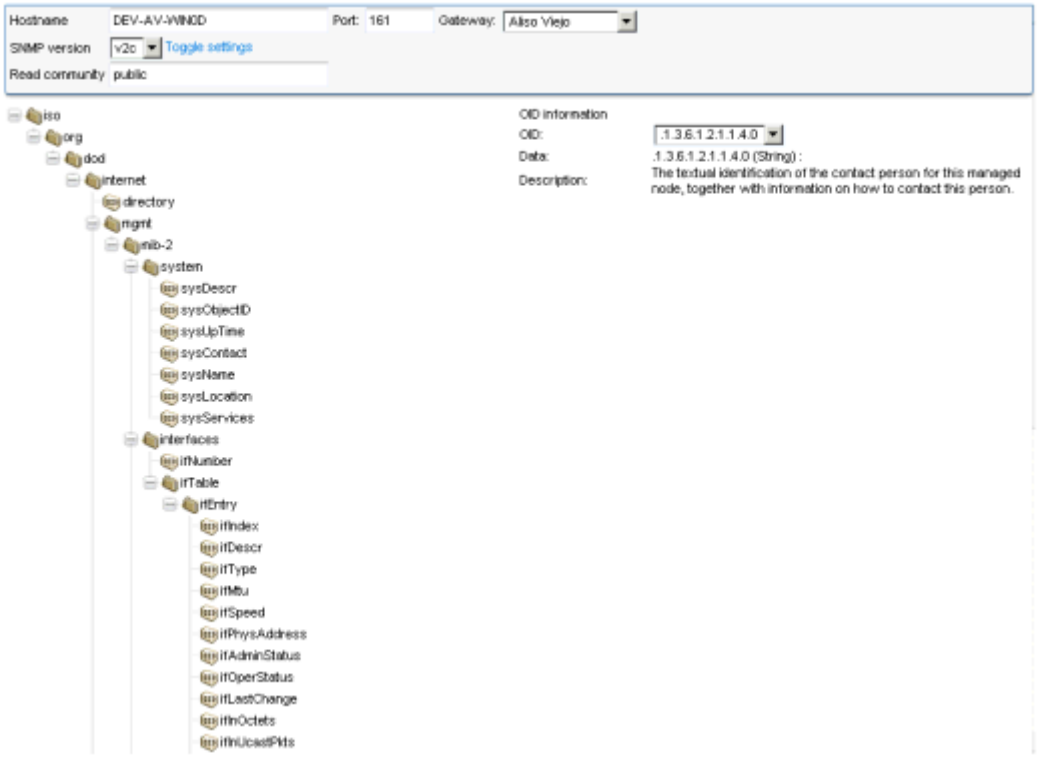
MIB-Baumstruktur

Hersteller haben versucht, die Identifikation der MIB-Objekte zu standardisieren, die in Geräten verwendet werden. Die MIB-Objekte werden dafür in einer MIB-Baumstruktur organisiert. Router beispielsweise können viele der gleichen MIB-Objekte verwenden und nur einige haben spezialisierte MIB-Objekte, die sich unterscheiden, um deren bestimmtes Produkt zu unterstützen.

Network Monitor zeigt die MIB-Baumstruktur in einem MIB Browser. Der MIB Browser kann mithilfe einer der folgenden Zugangsmethoden angezeigt werden:

- Network Monitor > Werkzeuge > MIB-Browser
- <Bestandsname> > Befehl-MIB Browser öffnen
- <Bestandsname> > Neuen Monitor hinzufügen > SNMP > OID [...]
- <Bestandsname> > Neuen Monitor hinzufügen > SNMP Trap > OID Einschließen/Ausschließen Filter [...]

Anhand der **MIB-Dateien, die auf dem Server installiert sind** *(siehe 99)* wird jederzeit der gleiche Strukturbaum angezeigt. Nachfolgend ist ein Beispiel eines MIB-Browser-Dialogs angezeigt.



Kompilieren von benutzerdefinierten MIB-Dateien

Sie können MIB-Dateien mit MIB-Compiler in ein binäres Format kompilieren, das **Network Monitor** lesen kann. Für das Kompilieren von MIB-Dateien ist ein Wissen über die Funktionsweise von MIB-Dateien sowie ein generelles Verständnis von SNMP und **MIB-Objekten** *(siehe 98)* erforderlich. Eine Anzahl verschiedener RFC-Dokumente stellen die Grundlage, auf der alle anderen MIB-Dateien basieren, dar.

> **Hinweis:** Der Communityname (SNMP-Version) und Port, der von **Network Monitor** verwendet wird, um eine Verbindung mit einem SNMP-Bestand zu erstellen, wird in der Registerkarte **Authentifizierung** *(siehe 40)* eines Bestandsknotens festgelegt. Der Bestandsknoten kann diese Einstellung von einem übergeordneten Knoten erben. Siehe **Installationscheckliste** *(siehe 4)*

Hierbei handelt es sich beispielsweise um die Kompilierungsreihenfolge des MIB eines CISCO®-Produkts.

1. `SNMPv2-SMI.mib`
2. `SNMPv2-TC.mib`
3. `SNMPv2-MIB.mib`
4. `RFC1213-MIB.mib`
5. `IF-MIB.mib`
6. `CISCO-SMI.mib`
7. `CISCO-PRODUCTS-MIB.mib`
8. `CISCO-TC.mib`

Die ersten fünf Dateien in diesem Beispiel sind für die meisten MiB-Dateien von Produkten einheitlich und werden in die standardmäßige binäre MIB-Datei `knm.mib` eingeschlossen.

> **Warnung:** Alle diese Dateien müssen gleichzeitig kompiliert werden, andernfalls schlägt der MIB-Compiler aufgrund ungelöster Symbole fehl.

Inhalt der standardmäßigen MIB-Datei von KNM

Die Standarddatei `knm.mib`, die in der Installation eingeschlossen ist, enthält die folgenden Basis OIDs (Objektbezeichner).

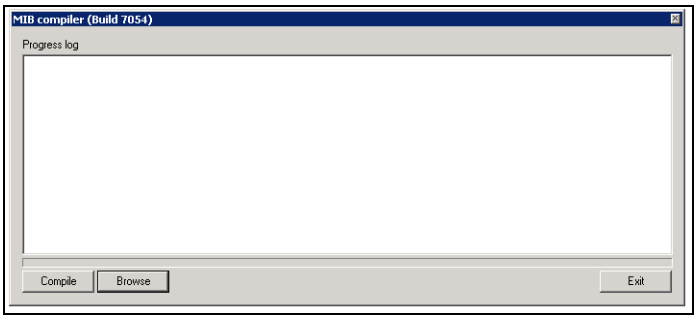
- `iso.org.dod.internet.directory`
- `iso.org.dod.internet.mgmt`
- `iso.org.dod.internet.experimental`
- `iso.org.dod.internet.private`
- `iso.org.dod.internet.security`

Die Datei befindet sich im Verzeichnis `\<KaseyaInstallDirectory>\KNM\mibs`.

Herunterladen und Ausführen des MIB-Compilers

1. Navigieren Sie zur Seite Network Monitor > Werkzeuge > **Downloads Dienstprogramme**.
2. Klicken Sie auf den Link des **MIB-Compilers**, um das Dienstprogramm auf den lokalen Rechner herunterzuladen.
3. Führen Sie das Dienstprogramm aus.

Kompilieren einer MIB-Datei



1. Starten Sie `<KaseyaInstallDirectory>\knm\mibcompiler.exe`.
2. Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine oder mehrere `*.mib` Dateien auszuwählen.
   - Suchen Sie die standardmäßige `knm.mib` Datei im `KNM\mibs`-Ordner des **Network Monitor**-Hostrechners. Doppelklicken Sie auf den Ordner, um ihn auszuwählen.
   - Wählen Sie alle zusätzlichen `*.mib` Dateien aus, die Sie in die Kompilierung einschließen möchten.
3. Klicken Sie auf die Schaltfläche **Kompilieren**.
4. Legen Sie fest, wo die kompilierte `*.dat` Datei gespeichert wird.
5. Klicken Sie auf die Schaltfläche **Durchsuchen**, um die `*.dat` Datei auszuwählen, die soeben kompiliert wurde. Eine interaktive MIB-Baumstruktur erscheint im Hauptfenster. Sie können diese verwenden, um zwischen den verschiedenen OIDs zu navigieren.
6. Verschieben oder kopieren Sie die kompilierte `*.dat` Datei in den Ordner `KNM\mibs`.

Datensatzmanagerprotokoll

Network Monitor > Werkzeuge > Datensatzmanagerprotokoll

Die Seite **Datensatzmanagerprotokoll** zeigt Protokolleinträge an, die durch den Service `Kaseya Record`

`Manager` erstellt wurden. Dieser Service wird bei der Installation von **Network Monitor** installiert. Die Funktion des Datensatzmanagers ist die statistische Datenspeicherung und Abfragefunktion für **Network Monitor**. Er basiert auf der gleichen Serviceklasse wie der Service `Kaseya Network Monitor`. Die gleichen Befehle für Installieren bzw. Deinstallieren funktionieren für beide.

Ordner

Datensatzmanager hat ein Basisverzeichnis, das in der Datei `rminit.cfg` festgelegt ist. Dieses Verzeichnis enthält einen Ordner für jeden Tag und einen Ordner mit dem Namen `realtime`. Der Ordner `realtime` enthält eine Anzahl von `X` Aufzeichnungen pro Monitor, um als Schnellzugriff-Cache zu dienen. Die XML-Datei kann neu erstellt werden.

rminit.cfg

Datensatzmanager hat eine "init"-Datei mit der Bezeichnung `rminit.cfg`, die die folgenden Parameter enthält:

```
# Record manager configuration file
bind_if=
listen_port=3030
storage_path=rmstorage
service_name=Kaseya Record Manager
display_name=Kaseya Record Manager
```

RPC

Datensatzmanager kommuniziert mit **Network Monitor** über RPC an Port 3030 (Standard) mithilfe des TCP/IP-Protokolls. Standardmäßig ist der Datensatzmanager im gleichen Verzeichnis wie `KNM` installiert. Bei Bedarf kann der Datensatzmanager auf einem anderen Gerät installiert werden.

Die KNM `init.cfg` Parameter müssen geändert werden, um diese Änderung geltend zu machen.

```
RECORDMGR_HOST=host_name_or_ip
RECORDMGR_PORT=3030
```

Mit Systemadministratorkonsole verwandte Befehle

Befehl	Schalter	Beschreibung
Status	-recordmgr	Druckt Statusmitteilung des Datensatzmanagers.
recordmgr-rebuild	JJJJ-MM-TT	Stellt die Datei für das angegebene Datum wieder her, z. B. 2012-09-01.
recordmgr-rebuild	-all	Stellt alle fertigen Dateien wieder her. Muss mit äußerster Vorsicht verwendet werden. Es kann mehrere Stunden dauern, bis dieser Vorgang abgeschlossen ist. Es ist möglich, dass in dieser Zeit Berichte nicht das richtige Ergebnis anzeigen.

Syslog-Meldung

Network Monitor > Werkzeuge > Syslog-Meldung

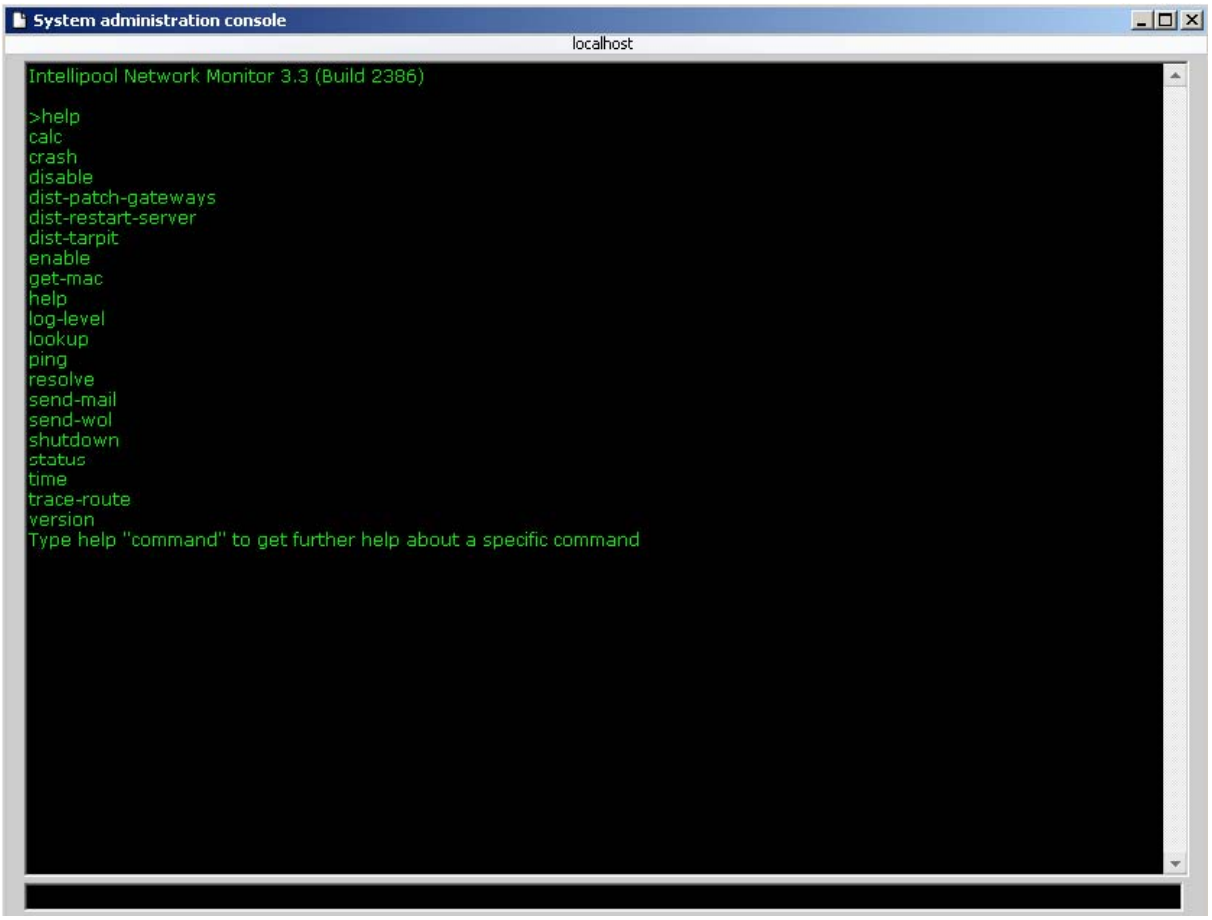
Auf der Seite **Letzte 50 Syslog-Meldungen** werden die letzten 50 Syslog-Meldungen angezeigt, die von allen **Network Monitor**Syslog**-Monitoren, die demselben Gateway angehören, an** *(siehe 146)* gesendet wurden.

Sie müssen das Sammeln von Syslog-Meldungen für jedes Gateway einzeln aktivieren, indem Sie das Kontrollkästchen Network Monitor > (ausgewähltes Gateway) > Bearbeiten > **Registerkarte "Erweitert"** *(siehe 38)* > **Syslog-Server** aktivieren.

Systemadministratorkonsole

Network Monitor > Werkzeuge > Systemadministratorkonsole

Die **Systemadministratorkonsole** dient dazu, die Erledigung regelmäßig wiederkehrender administrativer Aufgaben zu vereinfachen. Bei der Benutzeroberfläche handelt es sich um eine gewöhnliche Befehlszeilenschnittstelle, mit der die meisten Systemadministratoren vertraut sein dürften. Nur Benutzer, die als Systemadministratoren gekennzeichnet sind, haben Zugriff auf die Konsole.



Systemadministratorkonsole

Befehle

- `calc` – Ein integrierter Rechner für einfache Berechnungen. Verwendungsbeispiel:

```
calc 41+1
```

- `disable` – Deaktiviert eine Funktion in **Network Monitor**.
  - `-all` – Deaktiviert alle aufgelisteten Funktionen.
  - `-testing` – Deaktiviert Tests.
  - `-actions` – Deaktiviert die Ausführung von Aktionen.
  - `-statistics` – Deaktiviert die Speicherung von Statistiken.
  - `-login` – Deaktiviert den Login für normale Benutzer; Systemadministratoren können sich jedoch anmelden.
- `dist-patch-gateways` – Startet das Patchen aller Gateways, die ein Patchen erfordern.
- `dist-restart-server` – Startet den verteilten **Network Monitor**-Testserver neu.

- `dist-tarpit` – Fügt IP-Adressen zur Teergrube hinzu bzw. entfernt sie aus der Teergrube. Die Teergrube schützt den Server vor Brute-Force-Anmeldeversuchen und DoS-Angriffen.
  - `-block` – Blockiert die angegebene IP-Adresse.
  - `-unblock` – Hebt die Blockierung der angegebenen IP-Adresse auf.
  - `-list` – Listet alle IP-Adressen in der Teergrube auf.
  - `-blocktime` – Legt die standardmäßige Dauer der Blockierung in Minuten fest. Standardeinstellung: `20`.

```
dist-tarpit -block 192.168.0.1
```

- `enable` – Aktiviert eine Funktion in **Network Monitor**.
  - `-all` – Aktiviert alle aufgelisteten Funktionen.
  - `-testing` – Aktiviert Tests.
  - `-actions` – Aktiviert Aktionen.
  - `-statistics` – Aktiviert die Speicherung von Statistiken.
  - `-login` – Aktiviert den Login für normale Benutzer.
- `get-mac` – Ruft die MAC-Adresse für eine bestimmte IP-Adresse ab. Nur IPs im lokalen Netzwerk (LAN) des **Network Monitor**-Hostrechners können eine MAC-Adresse zurücksenden.

```
get-mac 192.168.42.1
```

- `help` – Zeigt hilfreiche Informationen zu den verschiedenen Befehlen in der Konsole an. Geben Sie `help <command>` ein, um sich eine Hilfe zu einem bestimmten Befehl anzeigen zu lassen.
- `log-level` – Passt die Protokollierungsstufe an. Wird **Network Monitor** neu gestartet, wird die Protokollierungsstufe standardmäßig auf den in der `init.cfg`-Datei festgelegten Wert zurückgesetzt. Gültige Werte sind 0, 1 und 2.
- `lookup` – Fragt einen DNS-Server nach Informationen zu einer Domain ab.

```
lookup kaseya.com
```

- `ping` – Pingt eine IP-Adresse oder einen Hostnamen.
- `resolve` – Löst einen Hostnamen in eine IP-Adresse auf.

```
resolve www.kaseya.com
```

- `send-mail` – Sendet über den integrierten **Network Monitor**-E-Mail-Client eine E-Mail an die angegebene Adresse.

```
send-mail myaddress@test.com , "Testing KNM" , "This is a test mail"
```

- `send-wol` – Sendet ein Wake-on-LAN-Paket an den angegebenen Host.

```
send-wol 192.168.42.1
```

- `shutdown` – Schließt **Network Monitor** und leert alle ungespeicherten Einstellungen von der Disk.
- `status` – Zeigt Informationen zum Status bestimmter Funktionen an.
  - `-thread` – Zeigt die aktuelle Anzahl aller Threads an, die von **Network Monitor** genutzt werden.
  - `-threadpool` – Zeigt die Gesamtzahl an Threads in einem Threadpool an.
  - `-memory` – Zeigt die aktuelle Speicherauslastung von **Network Monitor** an.
  - `-cpu` – Zeigt die aktuelle CPU-Auslastung von **Network Monitor** an.
  - `-handle` – Zeigt die aktuelle Handle-Auslastung von **Network Monitor** an.
  - `-feature` Zeigt den Status von **Network Monitor**-Funktionen an.
- `time` – Druckt Lokalzeit und -datum des **Network Monitor**-Hostrechners aus.
- `trace-route` – Führt eine Traceroute-Ermittlung zum angegebenen Host durch.
- `version` – Druckt die **Network Monitor**-Version aus. Kann auch dazu genutzt werden zu überprüfen, ob es eine neue Version von **Network Monitor** gibt.

```
version -check
```

Systemprotokoll

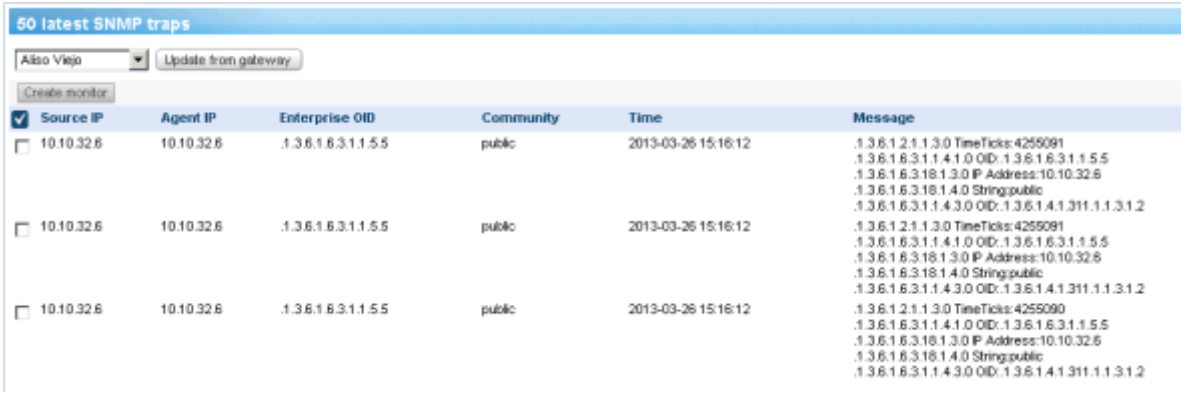
Network Monitor > Werkzeuge > Systemprotokoll

Die Seite **Systemprotokoll** zeigt Protokolleinträge an, die durch den Dienst `Kaseya Network Monitor` erstellt wurden. Es wird meistens verwendet, wenn ein Fehler aufgetreten ist. Sie können "ausführliche Protokollierung" aktivieren, indem Sie `LOG_LEVEL = 2` in der Datei `Init.cfg` (siehe 174) festlegen. Das ausführliche Systemprotokoll wird in einer separaten Textdatei gespeichert: `<Kaseya_Installation_Directory>\Logs\Services\KaseyaNetworkMonitor.log`.

Trap-Meldungen

Network Monitor > Werkzeuge > Trap-Meldungen

Auf der Seite **Letzte 50 SNMP-Traps** werden die letzten 50 SNMP-Trap-Meldungen angezeigt, die von den einzelnen Gateways empfangen wurden. Nutzen Sie diese Seite, um sicherzustellen, dass **Network Monitor** SNMP-Trap-Meldungen empfängt. **SNMP-Trap** *(siehe 142)*-Monitore können nur auf SNMP-Trap-Meldungen antworten, wenn die Meldungen auf dieser Seite angezeigt werden. Sie können diese Seite auch dazu nutzen, SNMP-Trap-Monitore für einen oder mehrere Bestände zu erstellen.



Aktionen

- **Von Gateway empfangene Meldungen aktualisieren** – Wählen Sie ein Gateway aus der Dropdownliste aus und klicken Sie auf **Von Gateway empfangene Meldungen aktualisieren**, um sich eine Liste der SNMP-Trap-Meldungen anzeigen zu lassen, die vom ausgewählten Gateway empfangen wurden.
- **Monitor erstellen** – Mithilfe dieser Option können Sie auf der Grundlage einer erhaltenen SNMP-Trap-Meldung **SNMP-Trap** *(siehe 142)*-Monitore für einen oder mehrere Bestände erstellen.

Eigene Einstellungen

Network Monitor > Werkzeuge > Eigene Einstellungen

Der aktuell angemeldete Benutzer kann Grundeinstellungen des eigenen Benutzerdatensatzes ändern. Die Eigenschaften sind in den folgenden Registerkarten geordnet:

- **Registerkarte "Basiseigenschaften"** *(siehe 105)*
- **Registerkarte "Benutzeroberflächenoptionen"** *(siehe 105)*

Registerkarte "Basiseigenschaften"

Network Monitor > Werkzeuge > Eigene Einstellungen > Registerkarte Basiseigenschaften

Basiseigenschaften

- **Benutzergruppe** – Zeigt die Benutzergruppen an, bei denen der aktuell angemeldete Benutzer Mitglied ist.
- **API-Schlüssel** – Eine numerische Zeichenfolge, die mit der Benutzeraufzeichnung verknüpft ist. Wird verwendet, um Anmeldungen durch Drittanbieter-Dienstprogramme zu authentifizieren, die eine Verbindung mit dem **Network Monitor**-Server herstellen. Eine neue, zufällig generierte Zeichenfolge kann durch Klicken auf die Schaltfläche **Neu** erstellt werden. Der API-Schlüssel wird durch das Dienstprogramm **Gizmo** *(siehe 207)* verwendet.
- **Nummer für SMS** – SMS-Benachrichtigungen für diesen Benutzer werden an diese SMS-Telefonnummer gesendet.

Registerkarte "Benutzeroberflächenoptionen"

Network Monitor > Werkzeuge > Eigene Einstellungen > Registerkarte Benutzeroberflächenoptionen

Benutzeroberflächenoptionen

- **Aktualisieren** – Gibt die Aktualisierungszeit (in Sekunden) für die Seiten in der Management-Benutzeroberfläche an.
- **Berichte anzeigen** - `Open reports in same window` oder `Open reports in a new window`.
- **Aktuellem Knoten folgen –** Wenn markiert, werden alle anderen Knoten geschlossen, wenn ein Knoten ausgewählt wird. Wird Option nicht markiert, bleiben alle anderen Knoten geöffnet, wenn ein Knoten ausgewählt wird.

Benutzerbenachrichtigungsgruppen

Network Monitor > Benutzer > Benutzerbenachrichtigungsgruppen

Die **Benutzergruppenliste** enthält Benutzergruppenbenachrichtigungen. Bestandsbenachrichtigungen werden an alle Mitglieder der Benutzergruppe gesendet, die mit diesem Bestand verknüpft sind. Dies erfolgt mithilfe der Einstellung **Benachrichtigung Benutzergruppe** in der **Registerkarte Basiseigenschaften** *(siehe 50)* des Bestands.

Aktionen

UMSCHALTTASTE + Klicken, um mehrere Zeilen auszuwählen. Geben Sie eine Zeichenfolge in das Suchfeld ein, um die Liste der angezeigten Aufzeichnungen zu filtern.

- **Löschen** – Löscht die ausgewählten Benutzergruppen.
- **(Bearbeiten)** – Klicken Sie auf das Symbol Eigenschaften, um eine einzelne Zeile zu bearbeiten.
- **Neue Gruppe** – **Eine neue Benutzergruppe erstellen** *(siehe 105)*.

Eine neue Benutzergruppe erstellen

Network Monitor > Benutzer > Benutzerbenachrichtigungsgruppen > Neue Gruppe oder Bearbeiten

Die Seite **Benutzergruppe bearbeiten** weist Benutzer einer Benutzergruppe zu.

Eigenschaften Benutzergruppe

- **Name** – Der Name der Benutzergruppe. Das sollte ein beschreibender Name sein.
- **Description** – Eine längere Beschreibung der Benutzergruppe.

Gruppenmitglieder

- **Benutzer** – Alle verfügbaren Benutzer in der VSA-Partition sind in diesem Feld aufgeführt. Um einen Benutzer zu der Benutzergruppe hinzuzufügen, wählen Sie ihn aus der Liste aus und klicken Sie auf die Schaltfläche **Markieren**.
- **Aktuelle Mitglieder** – Zeigt alle Benutzer an, die aktuell dieser Benutzergruppe hinzugefügt sind. Um einen Benutzer aus der Benutzergruppe zu entfernen, wählen Sie ihn aus der Liste aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Gruppenmanager** – Der Gruppenmanager legt einen Benutzer fest, dem die Funktion "Manager" der Benutzergruppe zugewiesen wird. Bei der Verwendung der Benutzerpläne zur Planung der Arbeitszeit eines Benutzers ist der Gruppenmanager standardmäßig der Kontakt, wenn kein anderer Benutzer verfügbar ist.

Angepasste Datentypen

VSA > Network Monitor > Einstellungen > Angepasste Datentypen

Die Seite **Angepasste Datentypen** ermöglicht die Erstellung benutzerdefinierter Datentypen für Monitore, die generische Daten speichern können. Zu diesen Monitoren gehören:

- CIM-Systemmonitor
- Datenbankmonitore (Datenbankserver, Oracle, MySQL, SQL-Server)
- Powershell-Skriptmonitor
- SNMP-Monitor
- SSH2-Skriptmonitor
- VMware-Systemmonitor
- Windows-Systemmonitor
- WMI-Monitor

Network Monitor ist mit vielen verschiedenen Datentypen vorkonfiguriert und kann diese für Reporting- und Darstellungszwecke optimal aufbereiten. In manchen Fällen kann es sinnvoll sein, dass Sie Ihre eigenen Datentypen definieren, z. B. wenn Sie mit geschützten Daten arbeiten.

Basiseigenschaften

- **Name** – Der Name des jeweiligen Datentyps.
- **Beschreibung** – Geben Sie eine Beschreibung des jeweiligen Datentyps ein.
- **Toplist** – Ist diese Option aktiviert, erscheint der jeweilige Datentyp als auswählbares Element unter den **Toplist** *(siehe 88)*-Berichtselementen.
- **Kompatible Monitore** – Die mit diesem Datentyp kompatiblen Monitortypen. Wählen Sie einen Monitortyp aus der Liste aus und klicken Sie die Schaltfläche **Auswählen** an. Einen ausgewählten Monitortyp können Sie aus der Auswahlliste entfernen, indem Sie ihn auswählen und die Schaltfläche **Entfernen** anklicken.
- **Gespeicherte Einheit** – Verwendet der jeweilige Datentyp eine oder mehrere Einheiten, müssen Sie angeben, welche Einheit von den Monitoren als Basiseinheit verwendet wird.
- **Kompatible Einheiten** – Wählen Sie Einheiten aus der Liste aus und ordnen Sie diese dem Datentyp zu. Diese Option ist beim Reporting von großem Nutzen, wenn Sie geschützte Daten in verschiedenen Einheiten anzeigen lassen möchten.

Einstellungen für die Darstellung

- **Dezimalstellen** – Geben Sie an, auf wie viele Dezimalstellen beim Anzeigen und beim Reporting dieses Datentyps gerundet werden soll.
- **Freistellen** – Geben Sie optional hohe oder niedrige Freistellungswerte für diesen Datentyp ein.

Bestandsvorlagen

Network Monitor > Einstellungen > Bestandsvorlagen

Auf der Seite **Bestandsvorlagen** können Sie für eine Gruppe von Monitoren – vergleichbar mit einem Bestand – Eigenschaften festlegen. Die Bestandsvorlage wird dann auf einen oder mehrere Bestände angewandt. Einen Monitor gleichzeitig für tausend Bestände zu konfigurieren, ist nicht praktikabel. Markieren Sie stattdessen eine vordefinierte Bestandsvorlage oder konfigurieren Sie Ihre eigene. Weisen Sie dann die Bestandsvorlage dem entsprechenden Bestand zu. Sie sollten für jeden Bestandstyp, den Sie verwalten, eine Bestandsvorlage haben. Siehe **Bestandsvorlagen** *(siehe 52)* für weitere Informationen.

Aktionen

- **Bearbeiten** - **Bearbeitet eine verlinkte Bestandsvorlage** *(siehe 107)*. Gilt nur für *benutzerdefinierte* Bestandsvorlagen, die unter Verwendung des Befehls **Als Vorlage speichern** *(siehe 52)* erstellt wurde, wenn ein Bestand ausgewählt wird.
- **Importieren** – Importieren Sie eine Bestandsvorlage aus einer externen XML-Datei.
  - Es ist möglich, eine Bestandsvorlagenkonfiguration von einer **Network Monitor**-Instanz in eine andere **Network Monitor**-Instanz zu importieren. Dies ermöglicht es der **Network Monitor**-Community, Monitoring-Lösungen gemeinsam zu nutzen.
  - Es ist möglich, ein Windows-Systemmonitorset oder ein SNMP-Set aus VSA zu exportieren und beim Import in eine Bestandsvorlagenkonfiguration umzuwandeln.
- **Löschen** – Löscht ausgewählte Bestandsvorlagen.
- – Bearbeiten Sie den Namen und die Beschreibung einer Bestandsvorlage.

Bearbeiten von Bestandsvorlagen

Network Monitor > Einstellungen > Bestandsvorlagen

Auf der Seite **Monitor-Konfiguration** können Sie die Liste der Monitore in einer Bestandsvorlage konfigurieren.

Aktionen

- **Löschen** – Löscht ausgewählte Monitore.
- **Neuer Monitor** – Fügt einen neuen Monitor hinzu.
- **Als XML exportieren** – Exportiert die Bestandsvorlage in eine externe XML-Datei. Exportierte Bestandsvorlagen enthalten niemals private Daten, wie z. B. Benutzernamen oder Kennwörter. Die in den exportierten Daten enthaltenen Informationen dienen der Monitorkonfiguration, enthalten aber keine Authentifizierungseinstellungen.
- **Aus XML aktualisieren** – Aktualisiert die Bestandsvorlage aus einer externen XML-Datei.
- **(klicken, um Monitor zu bearbeiten)** – Monitore innerhalb einer Bestandsvorlage werden größtenteils mit denselben Eigenschaften definiert wie unverknüpfte Monitore. Eine Beschreibung der Eigenschaften der verschiedenen Monitore finden Sie in der **Monitorreferenz** *(siehe 115)*.

Protokolleinstellungen

VSA > Network Monitor > Einstellungen >Protokolleinstellungen

Die Seite **Protokolleinstellungen** legt Protokollrichtlinien für **Network Monitor** fest. **Network Monitor**schreibt kontinuierlich ein Systemprotokoll, das Informationen über verschiedene Systemereignisse und andere Statusinformationen enthält. **Network Monitor**kann auch konfiguriert werden, sodass er Protokollinformationen an verschiedene Dienste sendet.

Protokollrichtlinien werden mithilfe der folgenden Registerkarten festgelegt.

- **Windows Ereignisprotokoll**
- **Syslog**
- **SNMP-Traps**
- **Speicherfrist**

Registerkarte "Windows Ereignisprotokoll"

- **Windows Ereignisprotokoll** – Bei Markierung speichert **Network Monitor** Protokollinformationen im Windows Ereignisprotokoll im `Application`-Protokollordner.

Registerkarte Syslog

- **Syslog** – Bei Markierung sendet **Network Monitor** Protokollinformationen an einen Syslog-Daemon. Geben Sie die Adresse und die Port-Nummer zu einem Host an mit einem laufenden Syslog-Server. Der **Network Monitor** Syslog-Client verwendet das UDP-Protokoll und Port `514` standardmäßig.
- **Syslog-Server** – Die Adresse des Syslog-Servers, der die Protokollinformationen empfängt.
- **Syslog-Port** – Die Port-Nummer des Syslog-Servers.

Registerkarte "SNMP-Trap"

- **SNMP-Trap** – Bei Markierung *sendet* **Network Monitor** alle Protokollinformationen als SNMP-Traps an eine Remote-Trap-Konsole.

> **Hinweis:** Kaseya hat eine benutzerdefinierte MIB-Datei erstellt, die von der Software importiert werden kann, die Traps von **Network Monitor** erhält. Die MIB-Datei mit dem Namen `knm.mib` befindet sich im Verzeichnis `\mibs`.

- **Trap-Empfänger** – Der Hostname oder die IP-Nummer des Trap-Empfängers.
- **Trap-Port** – Port-Nummer, den der Trap-Empfänger überwacht.
- **Community** – Die Community-Zeichenfolge des SNMP-Trap.

> **Hinweis:** Verwenden Sie die Registerkarte **Erweitert** eines **Gatewayknotens** *(siehe 37)*, um SNMP-Trap-Meldungen auf einem Netzwerk zu *erhalten*.

Speicherfrist

Gibt an, wie lange die Daten gespeichert werden sollen – `Forever`, `Month`, `Quarter`, `Year` – für das Folgende. `Month`, `quarter` und `year` stehen jeweils für eine bestimmte Anzahl an Tagen (30, 90 oder 365 Tage) ab dem aktuellen Datum.

- **Speicherfrist für Protokolle**
- **Speicherfrist für Datensätze**
- **Speicherfrist für Toplists**

NOC-Einstellungen

Network Monitor > Einstellungen > NOC-Konfiguration

Auf der Seite **NOC-Einstellungen** können Sie benutzerdefinierte NOC (Network Operations Center, dt. Netzwerkbetriebszentrum)-Ansichten erstellen. Diese Ansichten werden normalerweise im Vollbildmodus auf einem Monitor angezeigt.

Anweisungen zum Anzeigen einer NOC-Ansicht finden Sie in der Registerkarte **NOC** *(siehe 41)*.

Registerkarte "Allgemeine Einstellungen"

- **NOC-Ansichtsmodus** – Hierbei handelt es sich um eine globale Einstellung, die für alle NOC-Ansichten gilt. Ist die Option `View all monitor types` ausgewählt, sind alle Monitortypen in der NOC-Matrix zu sehen. Ist die Option `Hide unavailable monitor types` ausgewählt, sind nur diejenigen Monitortypen, die in einer bestimmten NOC-Ansichtskonfiguration enthalten sind, zu sehen, wenn die NOC-Ansicht angezeigt wird.

Registerkarte "Ansichtskonfiguration"

Mithilfe dieser Registerkarte können NOC-Ansichten konfiguriert werden. Um eine neue NOC-Ansicht zu erstellen, klicken Sie die Schaltfläche **Neue Ansicht** an. Um eine bestehende Ansicht zu bearbeiten, wählen Sie die jeweilige Ansicht aus der Liste aus und klicken Sie die Schaltfläche **Bearbeiten** an. Es können die folgenden Eigenschaften für eine NOC-Ansicht eingestellt werden:

- **Titel anzeigen** – Hierbei handelt es sich um den Titel der NOC-Ansicht, der oberhalb der NOC-Ansicht angezeigt wird.
- **Gruppieren nach** – Hier legen Sie fest, ob in der NOC-Ansicht Netzwerke, Bestände oder Bestände gefolgt von Monitoren angezeigt werden sollen.
- **Monitortypfilter** – Filtert die angezeigten Monitore nach Monitortypen.

Weitere Systemeinstellungen

Network Monitor > Einstellungen > Weitere Systemeinstellungen

Über die nachfolgend erläuterten Registerkarten der Seite **Weitere Systemeinstellungen** können Sie zusätzliche Einstellungen für Alarme und sonstige Ereignisse vornehmen.

- **Monitorstandardeinstellungen**
- **Datums- & und Wochenformat**
- **PageGate-Integration**
- **Weitere Einstellungen**

Monitorstandardeinstellungen

Diese Registerkarte enthält Standardeinstellungen für Monitorparameter, die dem Monitoring und der Speicherung statistischer Daten dienen.

- **Testintervall** – Das Standardabrufintervall für neue Monitore.
- **Alarmerzeugung** – Der Standardwert für die Erzeugung von Alarmen für neue Monitore.
- **Alarmtestintervall** – Das standardmäßig eingestellte Alarmtestintervall für neue Monitore.
- **Telnet-Eingabeaufforderung** – Geben Sie die entsprechenden Eingabeaufforderungen (getrennt durch Kommata) ein. Wenn **Network Monitor** sich an einem Telnet-Server anmeldet, muss ihm die Eingabeaufforderung bekannt sein.
- **Telnet-Anmeldeaufforderung** – Geben Sie die entsprechenden Anmeldeaufforderungen (getrennt durch Kommata) ein. Wenn **Network Monitor** sich an einem Telnet-Server anmeldet, muss ihm die Anmeldeaufforderung bekannt sein.

- **Telnet-Kennworteingabeaufforderung** – Geben Sie die entsprechenden Kennworteingabeaufforderungen (getrennt durch Kommata) ein. Wenn **Network Monitor** sich an einem Telnet-Server anmeldet, muss ihm die Kennworteingabeaufforderung bekannt sein.

Datums- & und Wochenformat

In dieser Registerkarte finden Sie Einstellungen für das Datums- und Wochenformat in **Network Monitor**.

- **Datumsformat** – Mithilfe dieser Einstellung können Sie Ihr bevorzugtes Datumsformat für die Anzeige des Datums in der Verwaltungsoberfläche und in Alarmmeldungen festlegen.
- **Wochenformat** – Mithilfe dieser Einstellung können Sie Ihr bevorzugtes Wochenformat festlegen.
- **Wochennummerierung** – Mithilfe dieser Einstellung legen Sie fest, auf welche Art und Weise in Ihrer Region die Wochen nummeriert werden.

PageGate-Integration

In dieser Registerkarte finden Sie Einstellungen für die Integration von PageGate in **Network Monitor**. Bei PageGate handelt es sich um eine von NotePage entwickelte Gateway-Anwendung für den SMS-Versand (**http://www.notepage.net** *(http://www.noteseite.net)*).

- **Schnittstellenmethode** – Wählen Sie die Schnittstellenmethode für die Kommunikation mit der PageGate-Software aus. Derzeit wird nur die `GetAscii`-Methode unterstützt.
- **Abrufverzeichnis** – Geben Sie hier an, welches Abrufverzeichnis für die `GetAscii`-Methode verwendet werden soll. Nähere Informationen hierzu finden Sie in den Begleitdokumenten der PageGate-Software.

SMS-Einstellungen

Network Monitor > Einstellungen > SMS > SMS-Einstellungen

Network Monitor kann SMS über ein Modem senden, das an die **Network Monitor**-Hostmaschine angeschlossen ist. Das Modem kann entweder ein GSM-Telefon oder ein Modem sein, das SMS über einen Festnetz-Dienstanbieter senden kann. Die Registerkarte **SMS-Einstellungen** konfiguriert die logischen Einstellungen, die für das Aktivieren der Verbindung erforderlich sind.

- **GSM-Telefon-Port** – Wählen Sie den Port aus der Liste der verfügbaren COM-Ports, um eine Verbindung zum Telefon herzustellen.
- **Baudrate** – Die Baudrate ist die Geschwindigkeit, mit der **Network Monitor** Daten liest und an das Modem überträgt. Lesen Sie das Handbuch zum Modem, um den richtigen Wert festzulegen. Es wird eine Einstellung von 2400 empfohlen, wenn Sie sich bei der Auswahl nicht sicher sind. *Bei der Auswahl einer falschen Baudrate kann es zu gelegentlichen Fehlern beim Senden von SMS-Nachrichten kommen.*
- **PIN-Code** – Feld für optionalen PIN-Code. Bei der Verwendung einiger GSM-Telefone muss **Network Monitor** einen PIN-Code senden, bevor eine Nachricht gesendet wird. Geben Sie den 4-stelligen PIN-Code in dieses Feld ein.

Konfigurieren des Modems

1. Wählen Sie den seriellen Port aus, mit dem das GSM-Modem verbunden ist.
2. Wählen Sie die Baudrate aus. Standardeinstellungen `9600`.
3. Geben Sie den PIN-Code ein, um die SIM-Karte zu entsperren (optional).
4. Klicken Sie auf die Schaltfläche **Speichern**, um die neuen Einstellungen zu speichern.

Telefonnummer des Benutzers

Es muss für jeden Benutzer eine SMS-Telefonnummer angegeben werden, der SMS-Benachrichtigungen von **Network Monitor** erhält. Gehen Sie dabei folgendermaßen vor:

- Network Monitor Eigene Einstellungen > **Registerkarte "Basiseigenschaften"** *(siehe 105)* > **SMS-Nummern**-Feld

Überprüfte SMS-Bestände

- Falcom Samba
- Falcom Swing
- Falcom Twist
- Nokia 30
- Z-text Festnetz-SMS-Modem

Die meisten modernen GSM-Telefone und Modems funktionieren in Kombination mit den hier aufgeführten Geräten. Der Bestand muss den SMS-Textmodus unterstützen und an einen COM-Port anzuschließen sein. Ein Bestand kann auch an einen USB-Port angeschlossen werden, aber der Bestands-Treiber muss den standardmäßigen seriellen Anschluss emulieren, sodass er durch **Network Monitor** erkannt werden kann.

Checkliste Installation des SMS-Modems

Der Bestand sollte an einen seriellen Port oder an den USB-Port mit serieller Emulation an die **Network Monitor**-Hostmaschine angeschlossen werden.

1. Schließen Sie das Telefonkabel an die **Network Monitor**-Hostmaschine an.
2. Installieren Sie den Modem-Treiber für Ihr Telefon (wenn erforderlich).
3. Mit einem Terminalprogramm mit dem Telefon verbinden.
4. Versuchen Sie, eine SMS zu senden, indem Sie Folgendes eingeben.
   - `ATZ`
   - `KNM SMS TEST`
   - `Press CTRL-Z`
   - `AT+CMGF=1`
   - `AT+CMGS="<PHONENUMBER>"`
5. Die SMS sollte jetzt gesendet werden. Beachten Sie, dass `<PHONENUMBER>` durch die Nummer des empfangenden Telefons ersetzt werden muss. Verwenden Sie Anführungszeichen (z. B. `"0068455"`). In der letzten Zeile müssen Sie die Tastenkombination `CTRL-Z` drücken.
6. Das Telefon sollte mit CMGS antworten, gefolgt von einer Nummer, die die ID der gesendeten SMS anzeigt.
7. Das Telefon ist jetzt bereit zur Verwendung mit **Network Monitor**.

CMS-Fehlercodes

8	Vom Betreiber festgelegte Sperre
10	Anruf gesperrt
21	Übertragung der Kurznachricht abgelehnt
27	Ziel außerhalb des Services
28	Unbekannter Teilnehmer
29	Funktion abgelehnt
30	Unbekannter Teilnehmer
38	Netzwerk außer Betrieb
41	Temporärer Fehler
42	Überlastung
47	Ressourcen nicht verfügbar, nicht festgelegt
50	Angeforderte Funktion nicht abonniert

69	Angeforderte Funktion nicht implementiert
81	Ungültiger Referenzwert für Übertragung der Kurznachricht
95	Ungültige Nachricht, nicht festgelegt
96	Ungültige erforderliche Informationen
97	Nachrichtentyp nicht vorhanden oder nicht implementiert
98	Nachricht nicht kompatibel mit Protokollstatus der Kurznachricht
99	Informationselement nicht vorhanden oder nicht implementiert
111	Protokollfehler, nicht festgelegt
127	Interworking, nicht festgelegt
128	Telematisches Interworking nicht unterstützt
129	Kurznachrichttyp 0 nicht unterstützt
130	Kann Kurznachricht nicht ersetzen
143	Nicht festgelegter TP-PID-Fehler
144	Datenkodierschema (Alphabet) nicht unterstützt
145	Nachrichtenklasse nicht unterstützt
159	Nicht festgelegter TP-DCS-Fehler
160	Befehl kann nicht ausgeführt werden
161	Befehl nicht unterstützt
175	Nicht festgelegter TP-Befehl-Fehler
176	TPDU nicht unterstützt
192	SC besetzt
193	Kein SC-Abonnement
194	SC-Systemfehler
195	Ungültige SME-Adresse
196	Ziel-SME blockiert
197	SM abgelehnt-Doppelte SM
198	TP-VPF nicht unterstützt
199	TP-VP nicht unterstützt
208	D0 SIM SMS-Speicher voll
209	Keine SMS-Speichermöglichkeit in SIM
210	Fehler in MS
211	Speicherkapazität überschritten
212	SIM-Anwendungs-Toolkit besetzt
213	Fehler beim Download der SIM-Daten
255	Nicht festgelegte Fehlerursache
300	ME-Fehler
301	SMS-Service von ME reserviert
302	Vorgang nicht zulässig.
303	Vorgang nicht unterstützt
304	Ungültiger PDU-Modus-Parameter
305	Ungültiger Textmodus-Parameter
310	SIM nicht eingefügt
311	PIN für SIM erforderlich

312	PIN für PH-SIM erforderlich
313	Fehler SIM
314	SIM besetzt
315	SIM falsch
316	PUK für SIM erforderlich
317	PIN2 für SIM erforderlich
318	PUK2 für SIM erforderlich
320	Fehler Speicher
321	Ungültiger Speicherindex
322	Speicher voll
330	SMSC-Adresse unbekannt
331	Kein Netzwerk-Service
332	Zeitlimit Netzwerk
340	KEINE +CNMA-BESTÄTIGUNG ERWARTET
500	Unbekannter Fehler
512	Durch Benutzer abgebrochen

Standardnachrichten

Network Monitor > Einstellungen > SMS > Registerkarte Standardnachrichten

Die Seite **Standardnachrichten** legt das Standardformat für Bestätigungsbenachrichtigungsmeldungen fest. *Dieses Format wird nicht für den Monitorbaum übernommen.*

> **Hinweis:** Das Thema **Alarmmeldungen** *(siehe 65)* führt die Formatvariablen auf, die in einer Bestätigungsbenachrichtigungsmeldung verwendet werden können.

Die Zeile **Betreff Bericht** gibt das Standardformat für eine E-Mail-Betreff-Zeile an, wenn ein erstellter Bericht per E-Mail an die Empfänger gesendet wird.

Monitorreferenz

Dieses Kapitel enthält Informationen zu *monitorspezifischen Einstellungen*. Siehe **Bearbeiten von Monitoren** *(siehe 61)* für Informationen zu *Standardmonitoreinstellungen*.

Monitore nach Betriebssystem

Die Monitortypen, die Sie einem Bestand hinzufügen können, richten sich nach dem **Betriebssystem**Betriebssystem, das für den Bestand bestimmt wurde. Üblicherweise wird das **Betriebssystem** eines Bestands während der **Netzwerkermittlung** *(siehe 23)* bestimmt. Sie können das **Betriebssystem** *(siehe 50)*, das für einen Bestand bestimmt wurde, manuell ändern. In der folgenden Tabelle wird aufgeführt, welche Betriebssystemtypen jeden Monitor unterstützten.

	Fenster	Linux/Unix	VMWare	Cisco, IOS-basiert	Andere/ Unbekannt
Active Directory *(siehe 117)*	●				
Bandbreitenauslastung *(siehe 118)*	●				
CIM-Monitor *(siehe 119)*		●	●		
Citrix-Server *(siehe 120)*	●	●	●	●	●
CPU-Auslastung *(siehe 120)*	●	●	●	●	
Datenbankserver *(siehe 121)*	●	●	●	●	●
Datenspeicherauslastung *(siehe 122)*			●		
DHCP-Abfrage *(siehe 123)*	●	●	●	●	●
Verzeichniseigenschaft *(siehe 123)*	●				
Plattenauslastung *(siehe 124)*	●	●	●	●	●
DNS-Suche *(siehe 125)*	●	●	●	●	●
Umgebungsmonitor *(siehe 126)*	●	●	●	●	●
Ereignisprotokoll *(siehe 126)*	●				
Exchange-Server *(siehe 127)*	●				

Dateiänderung *(siehe 128)*	●	●	●	●	●
FTP-Server *(siehe 129)*	●	●	●	●	●
IMAP4-Server *(siehe 129)*	●	●	●	●	●
JVM-Systemleistung *(siehe 129)*	●	●			●
LDAP-Abfrage *(siehe 131)*	●	●	●	●	●
Protokolldatei *(siehe 131)*	●	●	●	●	●
Lua-Skript *(siehe 132)*	●	●	●	●	●
Mail-Server QOS *(siehe 133)*	●	●	●	●	●
Speicherauslastung *(siehe 133)*	●	●	●	●	
MySQL *(siehe 134)*	●	●	●	●	●
NNTP-Server *(siehe 135)*	●	●	●	●	●
Oracle *(siehe 136)*	●	●	●	●	●
Ping *(siehe 137)*	●	●	●	●	●
POP3-Server *(siehe 138)*	●	●	●	●	●
Prozessstatus *(siehe 138)*	●	●	●	●	
RADIUS-Server *(siehe 139)*	●	●	●	●	●
Salesforce-Abfrage *(siehe 140)*	●	●	●	●	●
SMTP-Server *(siehe 141)*	●	●	●	●	●
SNMP *(siehe 141)*	●	●	●	●	●
SNMP-Trap *(siehe 142)*	●	●	●	●	●
SQL-Server *(siehe 143)*	●				
SSH2-Skript *(siehe 145)*	●	●	●	●	●
SSH2-Server *(siehe 145)*	●	●	●	●	●
Auslagerungsdateiauslastung *(siehe 146)*	●	●	●	●	
Syslog *(siehe 146)*	●	●	●	●	●
TCP-Port-Scan *(siehe 147)*	●	●	●	●	●
Telnet-Server *(siehe 147)*	●	●	●	●	●
Terminaldienst *(siehe 148)*	●	●	●	●	●
TFTP-Server *(siehe 148)*	●	●	●	●	●
Übertragungsgeschwindigkeit *(siehe 148)*	●	●	●	●	●
VMware-Systemleistung *(siehe 149)*			●		
Webserver *(siehe 150)*	●	●	●	●	●
Windows-Systemleistung *(siehe 151)*	●				
Windows-Dienststatus *(siehe 152)*	●				
WMI-Abfrage *(siehe 152)*	●				

Active Directory-Monitor

Der **Active Directory**-Monitor kann wichtige Aspekte eines Active Directory-Servers überwachen, wie z. B. die Replikationsverzögerung, die Domain-Controller-Zeitabweichung und die Verifizierung der Kerberos-Authentifizierung.

- Systemtyp: Fenster
- Kategorie: Verzeichnisdienst

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe auch **Standardmonitoreinstellungen** *(siehe 63)*.

Monitorvoraussetzungen

- Die Bestandsadresse muss der Name der Active Directory-Domäne sein, z. B. `mydomain.local`.
- Das Anmeldekonto muss ein Domänen-Benutzer sein.
- DCOM MUSS für die Active Directory-Überwachung aktiviert sein.
- Der KNM-Gateway-Rechner, der die Active Directory-Tests durchführt, MUSS selbst dem überwachten Active Directory angehören.
- Der Bestandsname MUSS der Domain-Name sein, NICHT der Name eines Bestands, wie z. B. eines Domain-Controllers. Der Active Directory-Bestand wird stattdessen alle zugewiesenen Domain-Controller aufzählen und bestimmte Aspekte dieser Domain-Controller aus dieser Liste überwachen.
- Das dem Bestand zugeordnete Windows-Konto MUSS ein Windows-Domain-Benutzer sein.
- Das dem Bestand zugeordnete Windows-Domain-Konto MUSS Lesezugriff auf alle überwachten Active Directory-Bestände haben.
- Um die Domain-Controller-Freigaben erfolgreich testen zu können, MUSS das Windows-Domain-Benutzerkonto, das dem Bestand zugewiesen ist, der Administratoren-, Hauptbenutzer-, Druck-Operatoren- oder Serverbenutzergruppe angehören.
- Das dem Bestand zugeordnete Windows-Domain-Benutzerkonto MUSS über die Berechtigung SE_TCB_NAME ("Einsetzen als Teil des Betriebssystems") verfügen, damit die Kerberos-Authentifizierung erfolgreich getestet werden kann.
- Für einen erfolgreichen Test des Globalen Katalogs ist EVENTUELL eine Kerberos-Authentifizierung erforderlich.

Monitorspezifische Eigenschaften

- **Anmeldekonto** – Das Anmeldekonto enthält die zu verwendenden Anmeldedaten für den Test des Active Directory-Servers. Das Anmeldekonto muss ein Domänen-Benutzer sein; anderenfalls schlägt der Test fehl.
- **Kerberos-Authentifizierung** – Ist diese Option aktiviert, wird getestet, ob das Active Directory erfolgreich eine Kerberos-Authentifizierung durchführen kann. Alle Authentifizierungsfehler werden in den Fehlerbericht aufgenommen und es wird ein Alarm ausgegeben.
- **Globaler Katalog** – Ist diese Option aktiviert, wird getestet, ob der Domain-Controller des Globalen Katalogs gefunden werden kann. Alle Fehler werden in den Fehlerbericht aufgenommen und es wird ein Alarm ausgegeben.
- **Im DNS veröffentlichte DCs** – Ist diese Option aktiviert, wird getestet, ob die Datensätze des Dienst-DNS-Servers des Domain-Controllers im DNS gefunden werden können (`"_ldap._tcp.DOMAIN."`, `"_kerberos._tcp.DOMAIN."`, `"_ldap._tcp.dc._msdcs.DOMAIN."`, `"_kerberos._tcp.dc._msdcs.DOMAIN."`, `"_ldap._tcp.Default-First-Site._sites.DOMAIN."` usw.).

- **Replikation** – Ist diese Option aktiviert, wird getestet, ob der letzte Replikationsversuch erfolgreich war.
- **Max. DC-Zeitabweichung** – Misst die Zeitabweichung zwischen Domain-Controllern in Sekunden. Übersteigt der Zeitunterschied zwischen den Domain-Controllern diesen Wert, schlägt der Test fehl.

LDAP-Abfrage

Optional kann eine LDAP-Abfrage ausgeführt und ihr Ergebnis im Rahmen eines Vergleichsvorgangs mit einem vordefinierten Wert verglichen werden.

- **LDAP-Abfrage** – Durchzuführende LDAP-Abfrage.
- **Vergleichswert** – Wert, mit dem das Abfrageergebnis verglichen werden soll.
- **Werttyp** – Typ des Werts, der mit dem aus der Datenbank abgerufenen Wert verglichen werden soll.
- **Vorgang** – Vorgang zur Bewertung des ausgegebenen Abfrageergebnisses und des Vergleichswerts, der dazu dient zu bestimmen, ob der Test erfolgreich war oder nicht.

Bandbreitenauslastungsmonitor

Der Bandbreitenauslastungsmonitor überwacht die Bandbreite an einer Netzwerkschnittstelle. Er kann mit oder ohne Schwellenwerteinstellungen konfiguriert werden. Bei Windows-Beständen kann die Bandbreite mittels *SNMP*, *WMI* oder *Windows-Leistungsindikatoren* gemessen werden. Für alle anderen Bestandstypen erfolgt die Messung mittels SNMP. **Verwenden Sie – wenn möglich – stets SNMP zur Überwachung der Bandbreite**, da es wesentlich schneller ist als die Messung der Bandbreite mittels WMI oder Windows-Leistungsindikatoren und zudem weniger Ressourcen in Anspruch nimmt.

- Für WMI oder Windows-Leistungsindikatoren ist ein Windows-Benutzer erforderlich, der Leseberechtigungen für die Registrierung des überwachten Bestands hat.
- Bei der Verwendung von Windows-Leistungsindikatoren muss der Dienst "Remoteregistrierung" aktiviert und auf dem überwachten Bestand gestartet sein.
- Wenn Sie Schwierigkeiten mit dem Monitortyp bei Windows-Rechnern haben, versuchen Sie diese durch Deaktivieren des Kontrollkästchens **WMI verwenden** in der **Registerkarte "Erweitert"** *(siehe 50)* des Bestandsknotens zu lösen.
- Der Communityname (SNMP-Version) und Port, der von **Network Monitor** verwendet wird, um eine Verbindung mit einem SNMP-Bestand zu erstellen, wird in der Registerkarte **Authentifizierung** *(siehe 40)* eines Bestandsknotens festgelegt. Der Bestandsknoten kann diese Einstellung von einem übergeordneten Knoten erben. Siehe **Installationscheckliste** *(siehe 4)*
- Systemtyp: Alle
- Kategorie: Leistung

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe auch **Standardmonitoreinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Schnittstellenname** – Anhand dieser Option können Sie die Schnittstelle für den Monitor auswählen.
- **Schnittstellengeschwindigkeit** – Optionaler Parameter zur manuellen Einstellung der Schnittstellengeschwindigkeit. Diese Einstellung kann nützlich sein, wenn Sie eine Netzwerkschnittstellenkarte überwachen, die an eine langsamere Verbindung, wie z. B. eine ADSL-Leitung angeschlossen ist. Die Geschwindigkeit ist stets in KB/Sek. anzugeben.
- **SNMP erzwingen** – Zeigt an, ob SNMP auf dem Bestand erkannt wurde. Ist die Option aktiviert, wird SNMP auch dann verwendet, wenn der Systemtyp des Bestands Windows ist.

- **Verknüpfungsstatus überprüfen** – Ist diese Option aktiviert, wird der `Up`- oder `Down`-Status überwacht. SNMP ist die einzige Methode, bei der das Kontrollkästchen **Verknüpfungsstatus überprüfen** aktiviert werden kann.
- **Einheit** – Einheit, in der die Daten zur Bandbreitenauslastung aufgezeichnet und angezeigt werden. Die Einheit kann nicht mehr geändert werden, sobald der Monitor erstellt wurde.
- **Schwellenwert** – Der obere Schwellenwert in der ausgewählten Einheit.
- **Anmeldedaten erben** – Legt die Anmeldedaten für die Windows-Domäne fest, falls erforderlich. Bei Markierung werden diese vererbt. Wenn dies deaktiviert ist, werden die Anmeldedaten für die Windows-Domäne, die in der Registerkarte **Authentifizierung** *(siehe 40)* für den Bestand festgelegt wurden, überschrieben.

CIM-Monitor

Der **CIM-Monitor** kann einen CIM-Agent (CIMOM) abfragen, der auf einer beliebigen Hardwareplattform konfiguriert ist, die CIM unterstützt und über den konfigurierten Agent und die konfigurierten Provider verfügt. Informationen zur Konfiguration des CIMOM finden Sie in Ihrem Hardwarehandbuch.

Der Monitor kann einen CIM-Leistungsindikator für einen CIMOM (Agent) abfragen und diesen im Rahmen eines Vergleichsvorgangs mit einem bestimmten Wert vergleichen. Ergibt der Vergleichsvorgang das Ergebnis "Falsch", schlägt der Monitortest fehl. Unterstützt werden die meisten Leistungsindikatorbestände, wie z. B. Hosts, Datenspeicher, Speicher, CPUs usw.

- Systemtypen: Linux/UNIX, VMware
- Kategorie: Leistung

Hinweis: Eine Einführung in die Verwendung des CIM-Monitors finden Sie in der Kaseya-**Knowledge Base** *(https://helpdesk.kaseya.com/entries/35975757)*.

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe auch **Standardmonitoreinstellungen** *(siehe 63)*.

Verbindungseinstellungen

- **Sichere HTTP-Verbindung (SSL) nutzen** – Es wird SSL für verschlüsselten Datenverkehr verwendet (Standard).

CIM-Monitoreigenschaften

- **Ziel-Namespace** – Standardeinstellung: `root/cimv2`. Informationen zu bestimmten Namespaces in Ihrem System finden Sie in Ihrem Hardwarehandbuch. Ein weiterer häufig vorkommender Namespace ist `root/interop`.
- **Klasse** – Klassen werden auf der Grundlage des von Ihnen gewählten Namespaces aufgeführt, sodass die Auflistung je nach System unterschiedlich aussehen kann.
- **Eigenschaft** – Die Art von Eigenschaft, die Sie überwachen möchten. Eigenschaften werden auf der Grundlage der von Ihnen gewählten Klasse aufgeführt.
- **Instanz** – Falls es mehrere Instanzen für die gewählte Klasse gibt, werden diese hier aufgeführt.
- **Divisor** – Das Ergebnis wird durch diesen Wert geteilt. Optional. Standardeinstellung: 1.
- **Datentyp** – Die Einheit der Daten, die im Rahmen des Tests aufgezeichnet werden. Dank dieser Einstellung ist es möglich, in Berichten Daten, die von diesem Monitortyp stammen, mit Daten anderer Monitortypen wie z. B. dem CPU-Auslastungsmonitor zu gruppieren.

Schwellenwerteinstellungen

- **Werttyp** – Typ des ausgegebenen Werts.
- **Vergleichsvorgang** – Vorgang zur Bewertung des ausgegebenen Ergebnisses und des vordefinierten Vergleichswerts.

- **Vergleichswert** – Benutzerdefinierter Vergleichswert. Es sind nur numerische Werte zulässig.

CIM-Konto

Wenn Sie "Sonstige/Unbekannt" als Bestandstyp gewählt haben, müssen Sie hier ein Konto für die Authentifizierung beim CIMOM wählen. *Stellen Sie sicher, dass Ihr CIM-Benutzerkonto zumindest über Lesezugriff auf den angegebenen Namespace verfügt.*

- **Anmeldedaten erben** – Ist diese Option aktiviert, werden die Anmeldedaten des Bestands vererbt. Wenn dies deaktiviert ist, geben Sie monitorspezifische Anmeldedaten ein.
- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diesen Monitor verwendet werden.
- **Port** – Standardmäßig auf 5989 (SSL) eingestellt. Der Standardport für unverschlüsselten Verkehr ist 5988.

Referenzen und Verknüpfungen

Bei CIM (Common Information Model) handelt es sich um einen Standard, der von der DMTF (Distributed Management Task Force) entwickelt und veröffentlicht wurde. Andere Standards wie WBEM (Web-Based Enterprise Management) definieren die Implementierung des CIM-Standards – einschließlich Protokolle für die Ermittlung und den Zugriff auf die Implementierungen.

Beispiele für Implementierungen sind WMI (Windows Management Instrumentation) und SBLIM (Standards Based Linux Instrumentation Management). Weitere Beispiele sind SMI-S (Storage Management Initiative – Specification), SMASH (Server Management Architecture for Server Hardware) und DASH (Desktop and mobile Architecture for System Hardware).

- http://en.wikipedia.org/wiki/Common_Information_Model_(computing)
- http://en.wikipedia.org/wiki/Windows_Management_Instrumentation
- http://sourceforge.net/apps/mediawiki/sblim/index.php?title=Main_Page
- http://en.wikipedia.org/wiki/Storage_Management_Initiative_-_Specification
- http://dmtf.org/standards/smash
- http://dmtf.org/standards/dash
- http://h18006.www1.hp.com/storage/smis.html – Auflistung von HP-Hardware, die SMI-S unterstützt.

Citrix-Servermonitor

Der **Citrix-Servermonitor** überprüft, ob ein Citrix-Server auf Verbindungsversuche reagiert.

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe auch **Standardmonitoreinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Port-Nummer** – Die Port-Nummer des Citrix-Dienstes.

CPU-Auslastungsmonitor

Dieser Monitor überwacht die **CPU-Auslastung** in einem Bestand und löst einen Alarm aus, falls der festgelegte Schwellenwert überschritten wird.

- Systemtyp: Alle außer Andere/Unbekannt

- Kategorie: Leistung

Bei Windows-Beständen sind die Methode zur Messung der CPU-Verwendung *WMI* oder *Windows-Leistungsindikatoren*.

- Für WMI oder Windows-Leistungsindikatoren ist ein Windows-Benutzer erforderlich, der Leseberechtigungen für die Registrierung des überwachten Bestands hat.
- Bei der Verwendung von Windows-Leistungsindikatoren muss der Dienst "Remoteregistrierung" aktiviert und auf dem überwachten Bestand gestartet sein.

Bei Unix-Beständen stellt KNM mit SSH2 eine Verbindung zu einem überwachten Bestand her und erzeugt Befehle, die für das ausgewählte Betriebssystem spezifisch sind. Stellen Sie sicher, dass der für UNIX-Bestände verwendete Benutzer die erforderlichen Befehle bearbeiten kann, wie z. B. `vmstat` oder `mpstat`. Installieren Sie falls erforderlich Systemtools für Ihr System, die das Dienstprogramm `mpstat` enthalten, um bestimmte CPUs oder Kerne zu überwachen. Andernfalls wird nur die Gesamtsystembelastung überwacht.

Hinweis: Wenn Sie Schwierigkeiten mit dem Monitortyp bei Windows-Rechnern haben, versuchen Sie diese durch Deaktivieren des Kontrollkästchens **WMI verwenden** in der **Registerkarte "Erweitert"** *(siehe 50)* des Bestandsknotens zu lösen.

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Max. CPU-Belastung** – Die maximale CPU-Verwendung in Prozent.
- **CPU-Nummer** – Die Nummer des CPUs auf dem Host. Dieser Wert wird in der Regel automatisch vom relevanten Bestand abgerufen. Um die Liste zu aktualisieren, drücken Sie auf den Link "CPU erneut suchen".
- **Detaillierter Fehlerbericht** (Nur Windows) – Bei Markierung sind die oberen fünf Prozesse der CPU-Auslastung enthalten.
- **Anmeldedaten erben** – Legt die Anmeldedaten für die Windows-Domäne fest, falls erforderlich. Bei Markierung werden diese vererbt. Wenn dies deaktiviert ist, werden die Anmeldedaten für die Windows-Domäne, die in der Registerkarte **Authentifizierung** *(siehe 40)* für den Bestand festgelegt wurden, überschrieben.

Datenbankservermonitor

Datenbankserver überwacht eine Datenbank mit ODBC. Der Test überprüft, ob die ODBC-Datenquelle geöffnet ist und auf sie zugegriffen werden kann. Der Monitor kann auch eine SQL-Abfrage ausführen und das Ergebnis mit einem vordefinierten Wert vergleichen.

- Systemtyp: Alle
- Kategorie: Datenbank

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Registerkarte "Grundlegend"

ODBC-Monitoreigenschaften

- **Datenquellenname** – Name der ODBC-Datenquelle, der für die Verbindung mit der Datenbank verwendet wird. Folgendes gilt für die Datenquelle:

- Sie muss auf dem System konfiguriert werden, *das den Gatewayknoten des Zielrechners hostet*.
- Es muss sich um eine ODBC-Datenquelle des DNS-Systemtyps handeln.
- Es muss sich um eine 32-Bit-Datenquelle handeln.
  - ✓ Auf 32-Bit-Gatewayhostsystemen muss `c:\Windows\System32\odbcad32.exe` ausgeführt werden, um die Datenquelle zu konfigurieren.
  - ✓ Auf 64-Bit-Gatewayhostsystemen muss `c:\Windows\SysWOW64\odbcad32.exe` ausgeführt werden, um die Datenquelle zu konfigurieren.

- **SQL-Abfrage** – Optionale SQL-Abfrage, die ausgeführt wird.

ODBC-Konto

- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des Bestands vererbt. Wenn dies deaktiviert ist, geben Sie monitorspezifische Anmeldedaten ein.

> **Hinweis:** Deaktivieren Sie dieses Kontrollkästchen für den Monitor und geben Sie monitorspezifische Anmeldedaten ein.

- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diesen Monitor verwendet werden.
- **Fehler bei fehlenden Zeilen** – Aktivieren Sie diese Option, damit der Monitor den Test nicht besteht, wenn bei der Abfrage keine Zeilen zurückgegeben werden.
- **Datentyp** – `SQL query value` ist die einzige aktuell unterstützte Option.

Schwellenwerteinstellungen

- **Werttyp** – Der Typ des Werts, der mit dem Wert, der von der Datenbank angefragt wird, verglichen wird.
- **Vorgang vergleichen** – Legen Sie fest, wie der angefragte Wert und der verglichene Wert für einen erfolgreichen Test in Beziehung stehen.
- **Vergleichswert** – Wert, mit dem das angefragte Ergebnis verglichen wird.

Datenspeicherauslastung

Datenspeicherauslastung überwacht freien Speicherplatz auf einem VMware-Datenspeicher und zählt automatisch verfügbaren Datenspeicher auf, der im Bestand überwacht werden muss.

- Systemtyp: VMware
- Kategorie: Leistung

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Datenspeichername** – Der Name des zu überwachenden Datenspeichers. Der Name wird automatisch vom Bestand abgerufen, wenn eine Bestandsüberprüfung ausgeführt wird. Um die Liste zu aktualisieren, drücken Sie auf den Link **Dienste erneut suchen**.
- **Freier Datenspeicher** – Mindestspeicherplatz, der auf dem in der Einheit unten ausgewählten Datenspeicher frei sein muss.
- **Einheit** – Wählen Sie die Einheit aus, die im Test verwendet wird. Der Schwellenwert für **Freier Datenspeicher** wird in dieser Einheit angegeben.

DHCP-Abfragemonitor

Der **DHCP-Abfragemonitor** überprüft, ob ein DHCP-Server IP-Adressen an Clients in einem Netzwerk leasen kann. Es muss mindestens eine Adresse frei sein, damit der Test erfolgreich ausgeführt werden kann.

- Systemtyp: Alle
- Kategorie: Directory Services

Network Monitor verwendet die MAC-Adresse der Netzwerkkarte, die zuerst auf dem **Gatewayhost** installiert wurde, um eine IP-Adresse vom DHCP-Server anzufragen.

- Der **Network Monitor**-Host kann DHCP nicht für die eigene Netzwerkschnittstelle verwenden, wenn dieser Monitor verwendet wird. Wenn der Gatewayhostrechner DHCP verwendet hat, ist ein mögliches Ergebnis, dass **Network Monitor** die IP-Adresse freigibt, die dem Host zugewiesen ist.
- Wenn der DHCP-Server auf einem anderen Netzwerk ist als der **Network Monitor**-Server, müssen Sie entweder ein Gateway auf diesem Netzwerk bereitstellen oder eine DHCP-Weiterleitung auf das Netzwerk einrichten, auf dem **Network Monitor** installiert ist (UDP-Hilfsprogramm).

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Verzeichniseigenschaftsmonitor

Der **Verzeichniseigenschaftsmonitor** kann die Dateianzahl, Verzeichnisgröße, relative Größenänderungen und das Dateialter in einem Verzeichnis testen. Der Testumfang kann auf Dateien begrenzt werden, die mit einem Platzhalter übereinstimmen.

- Systemtyp: Fenster
- Kategorie: Andere

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Freigabe** – Name der Freigabe in Beziehung zum Bestand. *Dateispezifikation ist erforderlich.* Formatierungsoptionen mit Platzhaltern sind zulässig. Zum Beispiel `\temp\*.?xt`. Weitere Formatierungsoptionen siehe unten.
- **OK bei fehlenden Dateien** – Bei Markierung der Option durchläuft der Monitor den Test erfolgreich, wenn keine übereinstimmenden Dateien vorhanden sind. Der Test wird erfolgreich durchgeführt, ohne die untergeordneten Tests zu prüfen.
- **Anmeldekonto** – Wählen Sie ein Konto aus der Liste aus, um das Standardkonto des Bestands zu überschreiben.
- **Max. Dateien** – Geben Sie die maximale Dateianzahl im Verzeichnis für den durchzuführenden Test an. Lassen Sie dies unausgefüllt, um den Test zu überspringen.
- **Min. Dateien** – Geben Sie die minimale Dateianzahl im Verzeichnis für den durchzuführenden Test an. Lassen Sie dies unausgefüllt, um den Test zu überspringen.
- **Max. Alter** – Geben Sie das Dateihöchstalter für die älteste Datei im Verzeichnis in Stunden und Minuten an. Zum Beispiel `HH:MM`. Lassen Sie dies unausgefüllt, um den Test zu überspringen.
- **Max. Alter neu** – Geben Sie das Dateihöchstalter für die aktuellste Datei im Verzeichnis an. Lassen Sie dies unausgefüllt, um den Test zu überspringen.

- **Rel. Schwellenwert** – Mit dem relativen Schwellenwerttest können Sie den aktuellen und den vorhergehenden Test auf relative Änderungen prüfen. Wählen Sie eine Option aus, durch die der Test fehlschlägt, wenn er als `true` ausgewertet wird.
- **Absoluter Schwellenwert** – Der absolute Schwellenwerttest kann verwendet werden, um die Verzeichnisgröße hinsichtlich eines absoluten Schwellenwerts in MB zu prüfen. Der Schwellenwert muss zusammen mit dem Vorgang als "wahr" ausgewertet werden, damit der Test erfolgreich durchlaufen wird.

Variablen für die Feldformatierung des Pfads

Die folgenden Formatierungsvariablen können verwendet werden, wenn der Pfad einer Freigabe festgelegt wird. Beispielsweise stimmt das Format `\sharename\*%[system.date_year]-%[system.date_month]-%[system.date_day_of_month].log` mit folgenden Dateinamen überein: `2013-01-15.log`, `2013-02-10.log`, `2013-03-06.log`.

- `%[system.time_hour]` – Stunde im 24-Stundenformat (00–23)
- `%[system.time_hour2]` – Stunde im 12-Stundenformat (01–12)
- `%[system.time_minute]` – Minute als Dezimalzahl (00–59)
- `%[system.time_second]` – Sekunde als Dezimalzahl (00–59)
- `%[system.date_year]` – Jahreszahl mit Jahrhundertangabe, als Dezimalzahl
- `%[system.date_year2]` – Jahreszahl ohne Jahrhundertangabe, als Dezimalzahl
- `%[system.date_month]` – Monat als Dezimalzahl (01–12)
- `%[system.date_day_of_month]` – Tag des Monats als Dezimalzahl (01–31)
- `%[system.date_day_of_year]` – Tag des Jahres als Dezimalzahl (001–366)
- `%[system.date_weekday]` – Wochentag als Dezimalzahl (0–6; Sonntag ist 0)

Plattenauslastungsmonitor

Plattenauslastung überwacht freien Speicherplatz auf einem Datenträger und zählt automatisch verfügbare Datenträger auf, die im Bestand überwacht werden müssen.

Bei Windows-Beständen sind die Methoden zur Messung der Plattenauslastung *WMI* oder *Windows-Leistungsindikatoren*.

- Für WMI oder Windows-Leistungsindikatoren ist ein Windows-Benutzer erforderlich, der Leseberechtigungen für die Registrierung des überwachten Bestands hat.
- Bei der Verwendung von Windows-Leistungsindikatoren muss der Dienst "Remoteregistrierung" aktiviert und auf dem überwachten Bestand gestartet sein.
- Wenn eine Windows-Freigabe statt eines Datenträgers oder eines Laufwerks überwacht wird, benötigt der Windows-Benutzer, der mit dem Bestand verknüpft ist, Netzwerklesezugriff auf den Freigabenamen.

Bei Unix-Beständen stellt KNM mit SSH2 eine Verbindung zu einem überwachten Bestand her und erzeugt Befehle, die für das ausgewählte Betriebssystem spezifisch sind. Stellen Sie sicher, dass der für UNIX-Bestände verwendete Benutzer erforderliche Befehle bearbeiten kann. `df`ist der Standardbefehl.

- Systemtyp: Alle außer Andere/Unbekannt
- Kategorie: Leistung

Hinweis: Wenn Sie Schwierigkeiten mit dem Monitortyp bei Windows-Rechnern haben, versuchen Sie diese durch Deaktivieren des Kontrollkästchens **WMI verwenden** in der **Registerkarte "Erweitert"** *(siehe 50)* des Bestandsknotens zu lösen.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Windows-Freigabe verwenden** – Diese Option wird nur für Bestände des Windows-Systemtyps angezeigt.
  - Bei Markierung verwendet der Monitor das SMB/CIFS-Netzwerkprotokoll, um die Plattenauslastung abzurufen. In diesem Fall müssen Sie einen Freigabenamen eingeben, zum Beispiel `C$`. Stellen Sie sicher, dass *Datei- und Druckerfreigabe* auf dem Bestand ausgeführt wird, wenn Sie diese Option aktivieren. Die Aufzählung von Datenträgern wird nicht unterstützt, wenn diese Option aktiviert ist.
  - Wenn dies deaktiviert ist, verwendet der Monitor die Windows-Systemleistungsregistrierung, um die Plattenauslastung abzurufen.
- **Datenträgername** – Der Name des zu überwachenden Datenträgers. Der Name wird automatisch vom Bestand abgerufen, wenn eine Bestandsüberprüfung ausgeführt wird. Um die Liste zu aktualisieren, drücken klicken Sie auf den Link **Disk-Volumes erneut suchen**. Wenn die Option **Windows-Freigabe verwenden** markiert ist, wird die Liste mit einem Textfeld ersetzt.
- **Freier Festplattenspeicher** – Mindestspeicherplatz, der auf dem in der Einheit unten ausgewählten Datenträger frei sein muss.
- **Einheit** – Wählen Sie die Einheit aus, die im Test verwendet wird. Der Schwellenwert **Freier Festplattenspeicher** wird in dieser Einheit angegeben
- **Anmeldedaten erben** – Legt die Anmeldedaten für die Windows-Domäne fest, falls erforderlich. Bei Markierung werden diese vererbt. Wenn dies deaktiviert ist, werden die Anmeldedaten für die Windows-Domäne, die in der Registerkarte **Authentifizierung** *(siehe 40)* für den Bestand festgelegt wurden, überschrieben.

DNS-Suchmonitor

Der **DNS-Suchmonitor** stellt eine Verbindung zum *auf dem Bestand ausgeführten DNS-Server* her und versucht die angegebenen Adressen in ein anderes Adressenformat zu übersetzen. Die eingegebenen Adressen können im Nummernformat (`255.255.255.255`) oder im Namensformat (`www.kaseya.com`) sein.

- Systemtyp: Alle
- Kategorie: Directory Services

Zum Testen umgekehrter DNS-Suchvorgänge müssen Sie sicherstellen, dass der DNS-Server, der vom KNM-Host oder vom Gateway verwendet wird, diese Funktion unterstützt. Überprüfen Sie dies mit dem Befehl `ping -a`.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Name** – Die Adresse, die für den Übersetzungstest verwendet wird. Trennen Sie die Adressen in diesem Feld mit einem Semikolon, um mehr als eine Adresse gleichzeitig zu testen.
- **Alle schlagen fehl** – Wenn diese Option markiert wird, müssen alle Adressen fehlgeschlagene Suchen haben, damit der Agent in einen fehlgeschlagenen Zustand übergeht.

Umgebungsmonitor

Der **Umgebungsmonitor** kann Hardware für das Monitoring von Umgebungsbedingungen überwachen. Es wird unterschiedliche Hardware von verschiedenen Herstellern unterstützt, einschließlich AKCP, IT Watchdogs, AVTECH, Sensatronics u. a.

- Systemtyp: Alle
- Kategorie: Umgebung

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorkonfiguration

Wenn ein neuer **Umgebungsmonitor** erstellt wird, muss der Benutzer zuerst den Hersteller und das Modell des Bestands auswählen. Sobald das Modell ausgewählt wurde, ruft **Network Monitor** automatisch die Bestandskonfiguration ab.

Monitorspezifische Eigenschaften

- **Temperatureinheit** – Die gewünschte Temperatureinheit für die Schwellenwertangabe. Dies hat auch einen Einfluss auf die visuelle Darstellung einer Echtzeitgrafik des Monitors.
- **Abrufmethode** – Diese Einstellung wählt die Abrufmethode für die Datenanfrage vom Bestand aus. Normalerweise muss dies nicht geändert werden.
- **Port** – Die Port-Nummer für den Datenabruf vom Bestand. Normalerweise wird dies von **Network Monitor** automatisch eingestellt.

Nach diesen allgemeinen Einstellungen, kann die Einstellung für jeden einzelnen Sensor am Bestand angegeben werden. Sie sind logisch in Gruppen angeordnete und entsprechen der Art, wie der Bestand zuvor konfiguriert wurde. Jeder Sensor muss durch Markieren des Aktivierungsfelds für jeden Sensor aktiviert werden. Schwellenwerte sind nicht erforderlich und können freigelassen werden, wenn der Sensor nur zur Erfassung von Statistiken verwendet wird.

Ereignisprotokollmonitor

Der **Ereignisprotokollmonitor** liest das Ereignisprotokoll und sucht nach Meldungen, die die Monitorparameter erfüllen. Es werden nur Ereignisprotokolleinträge in den aktuellen Test aufgenommen, die nach dem vorhergehenden Test erstellt wurden.

- Systemtyp: Fenster
- Kategorie: Protokoll

WMI wird für diesen Monitor verwendet, wenn **WMI verwenden** in der Registerkarte **Erweitert** des übergeordneten Bestands aktiviert ist. Deaktivieren Sie WMI, um Ereignisprotokolle unter `Applications and Services Logs` zu überwachen, da WMI nicht alle Protokolldateien lesen kann.

Wenn **WMI verwenden** nicht aktiviert ist, werden zwei unterschiedliche APIs für die Lesung der Ereignisprotokolle verwendet, je nach der Windows-Version. Die für Windows Vista/Server 2008 verwendete API unterscheidet sich von derjenigen, die für Windows Server 2003 oder Windows XP verwendet wird.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Ereignisquellenzeichenfolge** – (Optional) Die Ereignisquelle.

- **Computer** – (Optional) Der Computer, der den Protokolleintrag registriert hat.
- **Ereignis-ID** – Ereignis-ID-Nummer, für die ein Alarm ausgelöst wird. Trennen Sie mehrere Zahlen mit einem Komma voneinander. Lassen Sie das Feld leer, um alle Ereignis-IDs einzuschließen.
- **Ereignis-ID-Filter** – Ereignis-ID-Nummer der Ereignisse, die gefiltert werden. Trennen Sie mehrere Zahlen mit einem Komma voneinander.
- **Filter einschließen** – Wenn der Nachrichtentext der Ereignisdatei eine oder mehrere Zeichenfolgen enthält, wird der Datensatz dem Test hinzugefügt, wobei davon ausgegangen wird, dass alle anderen Kriterien erfüllt sind.
- **Filter ausschließen** – Wenn der Nachrichtentext der Ereignisdatei eine oder mehrere Zeichenfolgen enthält, wird der Datensatz dem Test **nicht** hinzugefügt, wobei davon ausgegangen wird, dass alle anderen Kriterien erfüllt sind.
- **Ereignistyp** – Der Ereignistyp, nach dem gesucht wird. Wenn die Alternative `all` ausgewählt wird, werden alle Ereignistypen für den Test berücksichtigt.
- **Nachricht einschließen** – Bei Markierung wird der Nachrichtentext im Fehlerbericht eingeschlossen.
- **Ereignisprotokoll** – Zeigt eine vordefinierte Liste der Protokollnamen an. Wählen Sie ein Protokoll für das Monitoring aus.
- **Alt. Ereignisprotokoll** – Alternativer Ereignisprotokollname. Geben Sie den Namen des zu suchenden Protokolls ein. Die Einstellung überschreibt die Einstellung für das **Ereignisprotokoll**.
- **Anmeldekonto** – Überschreibt das für einen Bestand ausgewählt Standardkonto.

Exchange-Servermonitor

Der **Exchange-Server-Monitortyp** kann E/A-Aktivitäten und E-Mail-Warteschlangen in der Größenordnung eines Microsoft Exchange 2007-Servers überwachen.

- Systemtyp: Fenster
- Kategorie: Internet und E-Mail

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Systemmonitoring

- **Byte gelesen/Sek.** – Der untere Schwellenwert für freien Speicher. Wenn der verfügbare Speicher unterhalb dieses Werts liegt, besteht der Monitor den Test nicht.
- **Byte geschrieben/Sek.** – Die Einheit des getesteten freien Speichers. Der Schwellenwert für freien Speicher wird in dieser Einheit angegeben.

Warteschlangenmonitoring

Lassen Sie diese Felder leer, um keine Tests durchzuführen.

- **Warteschlangengröße Senden (Postfach)** – Höchstanzahl der erlaubten Nachrichten in der Senden-Warteschlange von `mailbox`.
- **Warteschlangengröße Empfangen (Postfach)** – Höchstanzahl der erlaubten Nachrichten in der Empfangen-Warteschlange von `mailbox`.
- **Warteschlangengröße Senden (Öffentlich)** – Höchstanzahl der erlaubten Nachrichten in der Senden-Warteschlange von `public`.
- **Warteschlangengröße Empfangen (Öffentlich)** – Höchstanzahl der erlaubten Nachrichten in der Empfangen-Warteschlange von `public`.
- **SMTP-Kategorisierungs-Warteschlangengröße** – Höchstanzahl der erlaubten Nachrichten, die auf ihre Bearbeitung warten, wie z. B. Empfängerüberprüfung, Sortieren der lokalen oder Remoteübermittlung und die Erweiterung der Verteilerlistenempfänger. Viele wartende

Nachrichten in dieser Warteschlange können auf Leistungsprobleme in anderen Exchange-Komponenten oder in Active Directory hinweisen.

- **Nachrichten in Warteschlange für die Übermittlung** – Höchstanzahl der Nachrichten, die für die Übermittlung in die Warteschlange eingereiht werden.

Dateiänderungsmonitor

Der **Dateiänderungsmonitor** überprüft eine Datei auf Änderungen bezüglich der Größe oder des Änderungsdatums.

- Systemtyp: Alle außer Andere/Unbekannt
- Kategorie: Andere

Stellen Sie sicher, dass die verwendeten Benutzeranmeldedaten zumindest über Lesezugriff auf die überwachte Datei verfügen.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Windows-spezifische Eigenschaften

- **Dateipfad** – Der absolute Pfad der Datei mit UNC-Notation, einschließlich des Hostnamens. Auf diese Weise können Sie eine Zieldatei auf einem anderen Bestand auswählen als der Bestand, auf dem der Monitor eingerichtet ist. Zum Beispiel `\\myhost\c$\test.txt`

Unix-spezifische Eigenschaften

- **Dateipfad** – Pfad einer Datei, die relativ zum Host ist. Zum Beispiel `/home/robert/test.txt`

Monitorspezifische Eigenschaften

- **Datum** – Löst bei Markierung einen Alarm aus, wenn die Datei seit dem letzten Test geändert wurde.
- **Größere Größe** – Löst bei Markierung einen Alarm aus, wenn sich die Datei seit dem letzten Test vergrößert hat.
- **Kleinere Größe** – Löst bei Markierung einen Alarm aus, wenn sich die Datei seit dem letzten Test verkleinert hat.
- **Keine Veränderung** – Löst bei Markierung einen Alarm aus, wenn sich die Dateigröße oder das Datum seit dem letzten Test nicht geändert haben.

Pfad-Feldformatmarkierungen

Die folgenden Formatierungsvariablen können bei der Angabe eines Pfads eingeschlossen werden.

- `%[system.time_hour]` – Stunde im 24-Stundenformat (00–23)
- `%[system.time_hour2]` – Stunde im 12-Stundenformat (01–12)
- `%[system.time_minute]` – Minute als Dezimalzahl (00–59)
- `%[system.time_second]` – Sekunde als Dezimalzahl (00–59)
- `%[system.date_year]` – Jahreszahl mit Jahrhundertangabe, als Dezimalzahl
- `%[system.date_year2]` – Jahreszahl ohne Jahrhundertangabe, als Dezimalzahl
- `%[system.date_month]` – Monat als Dezimalzahl (01–12)
- `%[system.date_day_of_month]` – Tag des Monats als Dezimalzahl (01–31)
- `%[system.date_day_of_year]` – Tag des Jahres als Dezimalzahl (001–366)
- `%[system.date_weekday]` – Wochentag als Dezimalzahl (0–6; Sonntag ist 0)

FTP-Servermonitor

Der **FTP-Servermonitor** prüft, ob ein FTP-Server neue Verbindungen akzeptiert.

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

Der FTP-Servermonitor kann Dienstverfügbarkeit überwachen, die Anmeldung funktioniert jedoch ebenfalls. Geben Sie ein Konto für den Bestand oder den Monitor an. Wenn Sie sichergehen möchten, dass anonyme Logins funktionieren, verwenden Sie das "anonyme" Standardkonto. Die meisten FTP-Server akzeptieren einen beliebigen String oder Ihre E-Mail-Adresse als Kennwort.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Anmeldekonto** – Konto, das zur Anmeldung am FTP-Server verwendet wird. Wenn kein Anmeldekonto ausgewählt wird, wird eine einfache Port-Prüfung durchgeführt.
- **Port-Nummer** – Die Port-Nummer, die der FTP-Server überwacht.

IMAP4-Servermonitor

Der **IMAP4-Servermonitor** testet, ob er sich anmelden und ein Postfach auswählen kann. Der Test überprüft, ob der Teil zur Authentifizierung und zum Speichern des IMAP4-Servers funktioniert. Wenn kein Benutzername oder Kennwort angegeben ist, wird ein einfacher Verbindungstest durchgeführt.

- Systemtyp: Alle
- Kategorie: Internet und Mail

Fügen Sie entweder dem Objekt oder dem Monitor IMAP4-Anmeldedaten hinzu, um zu bestätigen, dass die Anmeldung funktioniert.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Benutzername/Kennwort** – Optionale Anmeldedaten zum Einloggen und Überprüfen des Postfachs
- **Posteingangsname** – Name des bei Angabe der Anmeldedaten zu überprüfenden Posteingangs
- **Port-Nummer** – Die Port-Nummer, die durch die Dienste überwacht wird.

JVM-Systemmonitor

Der **JVM-Systemmonitor** verwendet JMX zur Abfrage von Java Bean-Objekten und ihren Daten. Der Monitor vergleicht Java Bean-Werte mit einem Vergleichswert mithilfe eines Vergleichsvorgangs. Wenn der Vergleichsvorgang `false` ergibt, schlägt der Monitortest fehl. Optional können zwei Leistungsindikatoren abgefragt und kombiniert werden, bevor sie mit dem Vergleichswert verglichen werden.

- Systemtyp: Windows, Linux/UNIX, Sonstige/Unbekannt
- Kategorie: Leistung

Überwachen von durchschnittlicher CPU-Auslastung

Alle Bean-Objekte und deren Daten verwenden den **Datentyp** `Java VM performance data`, mit

Ausnahme der folgenden Einstellungskombinationen:

- **Objekt** – `java.lang.type=OperatingSystem`
- **Zähler** – `ProcessCpuTime`
- **Datentyp** – `CPU utilization`

In diesem Fall wird eine durchschnittliche CPU-Auslastung – ähnlich wie die CPU-Auslastung, die in JConsole angezeigt wird – durch das Abrufen von zwei Aufzeichnungen des `ProcessCpuTime`-Zählers mit einer dazwischen liegenden, bekannten Zeitverzögerung errechnet. Zeigt Daten optional in Prozent an.

Konfiguration

- Auf dem Java-Server muss JMX aktiviert und er muss über LAN zugreifbar sein.
- Auf dem **Network Monitor**-Gateway – einschließlich des lokalen Gateways auf dem **Network Monitor** Server-Computer – muss Oracle Java JDK (oder mindestens JRE) für 32-Bit-Anwendungen installiert sein. Wenn ein 64-Bit-Java-Programm installiert ist, entfernen Sie es vollständig oder löschen Sie es zumindest vollständig von der PATH-Umgebungsvariablen. Der Java-Installer kann von folgender Website heruntergeladen werden: **http://www.oracle.com/technetwork/java/javase/downloads/index.html** *(http://www.oracle.com/technetwork/java/javase/downloads/index.html)*.
- Wenn das Gateway x64 Windows ausführt und eine 32-Bit-Version von Java JRE (oder JDK) installiert wurde, gehen Sie zu Systemsteuerung > System > Erweiterte Systemeinstellungen und fügen Sie den folgenden String zur `PATH`-Umgebungsvariablen für den `system`-Benutzer hinzu.

  ```
  ;C:\Program Files (x86)\Java\jre7\bin;C:\Program Files
  (x86)\Java\jre7\bin\client
  ```

- Überprüfen Sie, ob der `%JAVA_HOME%\bin\client`-Ordner (wobei `%JAVA_HOME%` den Java-Installationsordner darstellt) die wichtige Datei `JVM.DLL` enthält, d. h. die **Network Monitor**Schnittstelle zu JNI und letztlich die Java VM.
- Starten Sie den Gatewayrechner neu, um sicherzustellen, dass die Einstellung auf allen laufenden Anwendungen und Diensten übernommen wird.
- Wenn JDK auf dem Gateway installiert ist, sollten Sie durch Ausführung der `JConsole.exe` (32-Bit)-Anwendung im Ordner JDK `bin` überprüfen, ob die Verbindung mit dem JMX-Server verfügbar ist.
- Stellen Sie sicher, dass das Gateway, einschließlich des KNM-Unterordners `local_gateway`, über seine eigene Kopie der JAR-Datei `jmx_connector.jar` verfügt, die sich im `KNM`-Installationsordner befindet.
- Stellen Sie beim Hinzufügen eines **JVM-Systemmonitors** sicher, dass das JVM-Konto – falls vorhanden – und die Porteinstellung auf die korrekten Werte eingestellt sind. Wählen Sie dann die Verknüpfung **ReScan** aus. Die Listenfelder **Objekt**, **Zähler** und **Instanz** werden mit verfügbaren Beans und seinen Datenfeldern gefüllt.

Monitorspezifische Eigenschaften

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

- **Objekt/Zähler/Instanz** – Name des zu testenden primären Leistungs-Bean. Diese Werte können mithilfe der Aufzählungsfunktion aufgezählt werden. Das Instanzfeld ist absichtlich bei manchen Zählertypen leer gelassen. Klicken Sie auf die Verknüpfung **Neu scannen**, um diese Werte zu aktualisieren.
- **Objekt/Zähler/Instanz** – Optional. Sekundäres Leistungs-Bean. Diese Werte können mithilfe der Aufzählungsfunktion aufgezählt werden. Das Instanzfeld ist absichtlich bei manchen Zählertypen leer gelassen.

- **Kombinationsvorgang** – Optionaler Vorgang, der bei Abfrage von zwei Zählern verwendet wird. Sie können mit dem Additions-, Subtraktions-, Divisions- oder Multiplikationsvorgang zu einem Endergebnis kombiniert werden.
- **Divisor** – Ein Wert, durch den der erhaltene Wert vor dem Vergleich dividiert wird.
- **Datentyp** – Die Dateneinheit, die durch den Test gesammelt wurden. Dadurch ist es möglich, Daten mit anderen Monitoren zu gruppieren, indem derselbe Typ für Berichte verwendet wird.
- **Werttyp** – Typ des Werts, der mit den abgefragten Daten verglichen wird.
- **Vergleichsvorgang** – Vorgang, der für Vergleiche verwendet wird.
- **Vergleichswert** – Wert, mit dem der Ergebniswert der Berechnung verglichen wird.
- **Anmeldedaten erben** – Legt die JVM-Anmeldedaten fest, falls erforderlich. Bei Markierung werden die Anmeldedaten geerbt. Wenn dies deaktiviert ist, werden die JVM-Anmeldedaten, die in der Registerkarte **Authentifizierung** *(siehe 40)* für den Bestand festgelegt wurden, überschrieben.
- **Port** – Die Port-Nummer des JVM-Dienstes.

LDAP-Abfragemonitor

Der **LDAP-Abfragemonitor** prüft, ob ein LDAP-Server auf eine Verzeichnissuchanfrage reagiert.

- Systemtyp: Alle
- Kategorie: Directory Services

Fügen Sie entweder dem Bestand oder dem Monitor LDAP-Anmeldedaten hinzu.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Benutzername/Kennwort** – Für die Suche verwendete Anmeldedaten. Wählen Sie ein Konto aus der Liste aus, um das Standardkonto des Bestands zu überschreiben.
- **Domain-Name** – Name der Domain oder Arbeitsgruppe, mit der der Benutzername verknüpft ist.
- **Port** – Port-Nummer, die der LDAP-Server überwacht.

Protokolldateimonitor

Der **Protokolldateimonitor** kann eine Textdatei lesen und auf *angehängte Zeilen prüfen, die eine der angegebenen Zeichenfolgen enthalten*. Der Monitor erzeugt einen Alarm, wenn die angegebenen Suchkriterien erfüllt werden. Der Monitor verwendet zur Verbindung mit einem Bestand SMB. Das bedeutet, dass nur die Anmeldedaten von Windows-Konten konfiguriert werden können. Sie müssen ein Windows-Konto einrichten, auch wenn das Zielbetriebssystem nicht Windows ist und Samba verwendet.

- Systemtyp: Alle
- Kategorie: Protokoll

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Pfad** – Der absolute Pfad der Datei, einschließlich Hostname. Zum Beispiel `\\myhost\C$\test.txt`.

- **Suchstring** – String, nach dem gesucht werden soll. Es kann nach mehreren Strings gesucht werden. Trennen Sie jeden Unterstring durch ein Komma. Wenn mehrere Unterstrings eingegeben werden, führt der Test eine logische "ODER'-Operation beim String durch.
- **Benachrichtigung bei keiner Änderung** – Bei Markierung schlägt der Test fehl, wenn die Datei sich seit dem letzten Test nicht geändert hat. Bei Markierung werden keine Suchstringtests durchgeführt.
- **Neu starten** – Bei Markierung startet der Monitor bei jedem Test oben in der Protokolldatei neu.
- **Anmeldedaten erben** – Wenn dies aktiviert ist, werden Anmeldedaten des Bestands vererbt. Wenn dies deaktiviert ist, geben Sie monitorspezifische Anmeldedaten ein.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diesen Monitor verwendet werden.

Pfad-Feldformatmarkierungen

Die folgenden Formatierungsvariablen können bei der Angabe eines Pfads eingeschlossen werden.

- `%[system.time_hour]` – Stunde im 24-Stundenformat (00–23)
- `%[system.time_hour2]` – Stunde im 12-Stundenformat (01–12)
- `%[system.time_minute]` – Minute als Dezimalzahl (00–59)
- `%[system.time_second]` – Sekunde als Dezimalzahl (00–59)
- `%[system.date_year]` – Jahreszahl mit Jahrhundertangabe, als Dezimalzahl
- `%[system.date_year2]` – Jahreszahl ohne Jahrhundertangabe, als Dezimalzahl
- `%[system.date_month]` – Monat als Dezimalzahl (01–12)
- `%[system.date_day_of_month]` – Tag des Monats als Dezimalzahl (01–31)
- `%[system.date_day_of_year]` – Tag des Jahres als Dezimalzahl (001–366)
- `%[system.date_weekday]` – Wochentag als Dezimalzahl (0–6; Sonntag ist 0)

Lua-Skriptmonitor

Der **Lua-Skriptmonitor** führt ein **Lua** *(siehe 205)*-Skript aus, das aus dem Ordner `KNM\script` des KNM-Hostrechners geladen wird.

- Systemtyp: Alle
- Kategorie: Skript

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Skript** – Wählen Sie das Skript aus der Liste aus. Die Liste basiert auf den Skripten, die im Ordner `\script` des KNM-Hostrechners gefunden werden.
- **Argument** – Argumente, die an das Skript weitergeleitet werden.
- **Anmeldekonto** – Optionale Anmeldedaten zur Windows-Authentifizierung, wenn bei dem Skript eine Authentifizierung erforderlich ist. Wählen Sie ein Konto aus der Liste aus, um das Standardkonto des Bestands zu überschreiben.
- **Nicht mit Konto anmelden** – Markieren Sie diese Option, wenn Sie die Authentifizierungsparameter zum Lua-Skript weiterleiten und dabei die Standardauthentifizierung umgehen möchten, die von **Network Monitor** vor dem Teststart durchgeführt wird.

Mailserver-QOS-Monitor

Der **Mailserver QOS-Monitor** testet die Fähigkeit eines Mailservers, E-Mails zu senden und zu empfangen. Statistiken zur Roundtrip-Dauer, zur Sendedauer und zur Anmeldungsdauer werden gespeichert.

- Systemtyp: Alle
- Kategorie: Internet und E-Mail

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Zeitlimit für E-Mail-Roundtrip** – Die maximale Dauer in Sekunden, die ein Monitor darauf wartet, dass eine E-Mail am POP3-Server ankommt.
- **SMTP-Server** – Die Adresse des SMTP-Servers, über den die Test-E-Mail gesendet wird.
- **SMTP-Port** – Die Port-Nummer des SMTP-Servers.
- **SMTP-Konto** – Optionales Konto, das zur Authentifizierung mit dem SMTP-Server verwendet wird. Wird ein Konto mit einem SMTP-Server ausgewählt, bei dem keine Authentifizierung erforderlich ist, schlägt der Test fehl. Lassen Sie dieses Feld leer, wenn Sie sich nicht sicher sind.
- **Absenderadresse** – E-Mail-Adresse, die im Feld "Absender" in der ausgehenden E-Mail verwendet wird.
- **Benutzerdefiniertes EHLO** – Der benutzerdefinierte EHLO-String, der zum Grüßen des Remote-E-Mail-Servers verwendet wird. Muss angegeben werden, wenn dieser Monitor einem Gateway zugewiesen ist.
- **POP3-Server** – Immer die Adresse des Bestands.
- **POP3-Port** – Die Port-Nummer des POP3-Servers.
- **E-Mail-Adresse** – Die E-Mail-Adresse, die im Test verwendet werden soll. Beachten Sie, dass die E-Mail-Adresse auf dem POP3-Server vorhanden sein muss und vom SMTP-Server zur Lieferung akzeptiert werden muss. Das E-Mail-Konto sollte exklusiv für **Network Monitor** sein, da der Test nach seinem Abschluss alle E-Mails löscht.
- **POP3-Konto** – Anmeldedaten, die zum Login auf dem POP3-Server verwendet werden.

Speicherauslastungsmonitor

Speicherauslastungsmonitor testet freien Speicher und löst einen Alarm aus, wenn der Speicherplatz unter dem angegebenen Schwellenwert liegt oder der Bestand nicht verfügbar ist.

- Systemtyp: Alle außer Andere/Unbekannt
- Kategorie: Leistung

Bei Windows-Beständen ist die Methode zur Messung der Speicherauslastung *WMI* oder *Windows-Leistungsindikatoren*.

- Für WMI oder Windows-Leistungsindikatoren ist ein Windows-Benutzer erforderlich, der Leseberechtigungen für die Registrierung des überwachten Bestands hat.
- Bei der Verwendung von Windows-Leistungsindikatoren muss der Dienst "Remoteregistrierung" aktiviert und auf dem überwachten Bestand gestartet sein.

Bei Unix-Beständen stellt KNM mit SSH2 eine Verbindung zu einem überwachten Bestand her und erzeugt Befehle, die für das ausgewählte Betriebssystem spezifisch sind. Stellen Sie sicher, dass der für UNIX-Bestände verwendete Benutzer erforderliche Befehle bearbeiten kann. `free -m` ist der Standardbefehl. Es kann eine Softwareinstallation auf Ihrem Bestand erforderlich sein.

Hinweis: Wenn Sie Schwierigkeiten mit dem Monitortyp bei Windows-Rechnern haben, versuchen Sie diese durch Deaktivieren des Kontrollkästchens **WMI verwenden** in der **Registerkarte "Erweitert"** *(siehe 50)* des Bestandsknotens zu lösen.

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Freier Speicher** – Die erforderliche Menge an freiem Speicher. Wenn der freie Speicher unterhalb dieses Werts liegt, schlägt der Monitortest fehl.
- **Einheit** – Die Einheit des getesteten freien Speichers. Der Schwellenwert für freien Speicher wird in dieser Einheit angegeben.
- **Prozessbericht** – Bei Markierung ist in der Alarmmeldung auch die Speichernutzung bei Prozessen enthalten.
- **Task-Manager-Annäherung** – Bei Markierung wird die Speicherauslastung mit einer Methode berechnet, die sich den Werten des Windows Task-Managers annähert. Ist diese Option nicht markiert, wird eine Legacy **Network Monitor**-Methode verwendet.
- **Anmeldedaten erben** – Legt die Anmeldedaten für die Windows-Domäne fest, falls erforderlich. Bei Markierung werden diese vererbt. Wenn dies deaktiviert ist, werden die Anmeldedaten für die Windows-Domäne, die in der Registerkarte **Authentifizierung** *(siehe 40)* für den Bestand festgelegt wurden, überschrieben.

MySQL-Monitor

Dieser **MySQL**-Monitortyp kann mehrere Schlüsselaspekte einer MySQL-Datenbank überwachen.

- Systemtyp: Alle
- Kategorie: Datenbank

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Voraussetzungen

Es müssen die Pakete **MySQL Connector/C** *(http://www.mysql.com/downloads/connector/c)* oder **MySQL Workbench** *(http://dev.mysql.com/downloads/tools/workbench/5.2.html)* auf dem **Network Monitor**-Server oder Gateway installiert sein. Laden Sie den 32-Bit-Client herunter, auch wenn Ihr Server eine 64-Bit-Version ist. Der Grund dafür ist, dass **Network Monitor** eine 32-Bit-Anwendung ist und 32-Bit-Treiber benötigt.

Stellen Sie nach der Installation sicher, dass sich der Dateipfad zu `libMysql.dll` im Windows-Dateipfad befindet. Dies geschieht normalerweise während der Installation des Administratorpakets und es kann ein Neustart des Servers erforderlich sein. Der **Network Monitor** `nmservice.exe`-Dienst muss neu gestartet werden, damit die Änderung gültig wird. Wenn **Network Monitor** nicht auf diese DLL-Datei zugreifen kann, schlägt der MySQL-Monitor mit einer Fehlermeldung fehl und gibt an, dass er die `libMysql.dll`-Datei nicht finden kann.

Wenn Ihr MySQL-Server normalerweise nur auf lokale Abfragen reagiert, d. h. Ihre Anwendung sich auf demselben Server wie die Datenbank befindet, können Sie mit diesen einfachen Schritten KNM dazu bringen, Ihre MySQL-Datenbank zu überwachen.

- Ihr MySQL-Server muss auf Anfragen von einem Remote-Host reagieren. Standardmäßig lautet die Bind-Adresse 127.0.0.1, also müssen Sie "bind-address" in `/etc/mysql/my.cnf` auf die korrekte IP-Adresse Ihres Servers ändern oder die Zeile mit # vor der Zeile `bind_address` kommentieren, damit der Server alle IP-Adressen Ihres Servers überwacht.

- Standardmäßig ist es Ihrem Client möglicherweise nicht gestattet, sich mit Ihrer Datenbank zu verbinden. Mit den folgenden Schritte erlauben Sie Ihrem Client, eine Verbindung zur Datenbank herzustellen:
  1. SSH zu Ihrem MySQL-Server
  2. `mysql –u root –p`
     Kennwort eingeben
  3. Die folgende Abfrage durchführen:

     ```
     use <database name>
     GRANT ALL ON *.* to root@'<ip address of your KNM host/gateway>' IDENTIFIED
     BY '<your root password>';
     FLUSH PRIVILEGES;
     ```

Monitorspezifische Eigenschaften

Diese Felder sind erforderlich, um eine Verbindung zur Datenbank herzustellen und konfigurierte Tests durchzuführen.

- **Anmeldekonto** – Das Anmeldekonto enthält die zu verwendenden Anmeldedaten für die Authentifizierung mit der MySQL-Datenbank.
- **Port** – Port-Nummer, die der Datenbankserver überwacht.
- **Datenbankname** – Name der Datenbank, zu der eine Verbindung hergestellt wird.

Systemmonitoroptionen

Lassen Sie diese Felder leer, um keine Tests durchzuführen.

- **Max. Thread-Anzahl** – Ein numerischer Wert, der die maximale Anzahl laufender Threads darstellt. Wenn die Anzahl der laufenden Threads diesen Wert übersteigt, schlägt der Monitortest fehl.
- **Max. Replikationslatenz** – Ein Wert in Sekunden, der die maximale Zeitdifferenz zwischen Master und Slave wiedergibt. Wird dieser Wert überschritten, schlägt der Monitortest fehl.
- **Max. langsame Abfragen** – Eine langsame Abfrage ist als eine Abfrage definiert, die länger als die Durchschnittszeit ausgeführt wurde und die in der Datenbankkonfiguration definierte `long_query_value`-Zeit überschreitet. Geben Sie einen numerischen Schwellenwert ein, damit der Test fehlschlägt, wenn die Anzahl der langsamen Abfragen diesen Wert übersteigt.
- **Max. offene Tabellen** – Ein numerischer Wert, der die maximale Anzahl erlaubter offener Tabellen angibt.
- **Durchschnittliche Abfragen pro Sekunde** – Ein numerischer Wert, der die maximale Anzahl erlaubter ausgeführter Abfragen pro Sekunde angibt.
- **Max. Benutzer** – Max. Anzahl der Benutzer, die gleichzeitig angemeldet sein dürfen.

SQL-Abfrageoption

Eine optionale SQL-Anweisung kann ausgeführt und ihre Ausgabe mit einem vordefinierten Wert mithilfe einer Vergleichsoperation verglichen werden.

- **SQL-Abfrage** – Optionale SQL-Abfrage, die ausgeführt wird.
- **Fehler bei keiner Zeile** – Aktivieren Sie diese Option, damit der Monitortest fehlschlägt, wenn bei der Abfrage keine Zeilen zurückgegeben werden.
- **Vergleichswert** – Wert, mit dem das Abfrageergebnis verglichen wird.
- **Werttyp** – Typ des Werts, der mit dem aus der Datenbank abgerufenen Wert verglichen wird.
- **Vorgang** – Vorgang zur Bewertung des ausgegebenen Abfrageergebnisses und des zu bestimmenden Vergleichswerts, wenn der Test erfolgreich war oder fehlgeschlagen ist.

NNTP-Servermonitor

Der **NNTP-Servermonitor** stellt eine Verbindung her und überprüft den Status eines NNTP (Network

News Transport Protocol)-Servers.

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Port-Nummer** – Die Port-Nummer, für deren Verwendung der NNTP-Server konfiguriert ist.

Oracle-Monitor

Dieser **Oracle**-Monitortyp kann mehrere wichtige Aspekte einer Oracle-Datenbank überwachen. Der Monitor verwendet die native Oracle-Schnittstelle und es muss kein ODBC-Treiber auf dem **Network Monitor**-Hostrechner installiert werden.

- Systemtyp: Alle
- Kategorie: Datenbanken

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Voraussetzungen

Installieren Sie den **Oracle Database Instant Client** *(http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html)* auf dem **Network Monitor**-Server oder Gateway. Laden Sie den 32-Bit-Client herunter, auch wenn Ihr Server eine 64-Bit-Version ist. Grund dafür ist, dass **Network Monitor** eine 32-Bit-Anwendung ist und 32-Bit-Treiber benötigt.

Stellen Sie nach der Installation sicher, dass der Ordner, in dem das Paket installiert wurde, sich im Windows-Systempfad befindet. Dazu könnte ein Neustart des Servers erforderlich sein. Starten Sie nach Änderung des Systempfads den **Network Monitor**-Dienst neu, damit die Änderung gültig wird. Wenn **Network Monitor** nicht auf die benötigten DLL-Dateien zugreifen kann, schlägt der Oracle-Monitor mit einer Fehlermeldung fehl und gibt an, dass er die DLL-Dateien nicht finden kann.

Oracle-Konto

Diese Felder sind erforderlich, um eine Verbindung zur Datenbank herzustellen und konfigurierte Tests durchzuführen.

- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des Bestands vererbt. Wenn dies deaktiviert ist, geben Sie monitorspezifische Anmeldedaten ein.
- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diesen Monitor verwendet werden.
- **Dienstname** – Der Name des Dienstes, der im Feld `tnsnames.ora` definiert ist. **Network Monitor**verwendet diese Informationen, um eine Verbindung mit der Oracle-Datenbank herzustellen.
- **Port** – Die Port-Nummer, die der Oracle-Datenbankserver überwacht.

Systemmonitoroptionen

- **Max. offene Cursors** – Ein numerischer Wert, der die maximale Anzahl gleichzeitig offener Cursors angibt. Wenn die Anzahl der offenen Cursors diesen Werte übersteigt, schlägt der Monitortest fehl. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.

- **Schwellenwert Vorgangslänge** – Ein Wert in Sekunden, der die maximale Dauer angibt, die ein Vorgang ausgeführt werden kann. Wird diese Dauer überschritten, schlägt der Monitortest fehl. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.
- **Puffer-Cache-Trefferverhältnis** – Das Puffer-Cache-Trefferverhältnis gibt den Prozentsatz von der Gesamtzahl an Anfragen an, die ohne Zugriff auf den Datenträger bedient wurden. Ein höherer Wert bedeutet eine bessere Datenbankleistung. Stellen Sie diesen Wert auf den niedrigsten akzeptablen Wert ein. Wenn die Quote unter diesen Wert fällt, schlägt der Monitortest fehl. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.
- **Fehlgeschlagene Anmeldungen** – Ein numerischer Wert, der die maximale Anzahl erlaubter fehlgeschlagener Anmeldungen an einem Tag angibt. Um diesen Wert zu testen, muss Audit aktiviert sein. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.

Optionen der Tabellenbereichsüberwachung

Ein Tabellenbereich ist mit physikalischen Dateien verknüpft, die auf einer Disk gespeichert sind. Jede Datenbank kann mit einem oder mehreren Tabellenbereichen zur Speicherung von Tabellen und Indizes verknüpft werden. Durch Überwachung der Tabellenbereichsnutzung können Sie gewarnt werden, bevor der verbleibenden Speicherplatz in einem Tabellenbereich einen Schwellenwert unterschreitet.

- **Tabellenbereichsnutzung** (beliebig) – Ein Schwellenwert, der die maximal erlaubte Nutzung eines Tabellenbereichs in Prozent angibt. Dieses Feld gilt für alle Tabellenbereiche in der Datenbank. Nachfolgende Felder können verwendet werden, um Ausnahmen für diese Regel zu konfigurieren, für bis zu fünf andere Tabellenbereiche. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.
- **Tabellenbereichsnutzung** (1–5) – Ein Schwellenwert für die maximal erlaubte Nutzung eines bestimmten Tabellenbereichs. Diese Felder überschreiben den globalen Tabellenbereichs-Schwellenwert. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.

SQL-Abfrageoption

Eine optionale SQL-Anweisung kann ausgeführt und ihre Ausgabe mit einem vordefinierten Wert mithilfe einer Vergleichsoperation verglichen werden.

- **SQL-Abfrage** – Optionale SQL-Abfrage, die ausgeführt wird.
- **Fehler bei fehlenden Zeilen** – Aktivieren Sie diese Option, damit der Monitor den Test nicht besteht, wenn bei der Abfrage keine Zeilen zurückgegeben werden.
- **SYSDBA-Berechtigung** – Bei Markierung werden die Anmeldedaten auf SYSDBA angehoben.
- **Werttyp** – Typ des Werts, der mit dem aus der Datenbank abgerufenen Wert verglichen wird.
- **Vergleichsvorgang** – Vorgang zur Bewertung des ausgegebenen Abfrageergebnisses und des zu bestimmenden Vergleichswerts, wenn der Test erfolgreich war oder fehlgeschlagen ist.
- **Vergleichswert** – Wert, mit dem das Abfrageergebnis verglichen wird.

Ping-Monitor

Ping-Monitor verwendet das ICMP-Protokoll, um zu überprüfen, ob der Bestand auf Ping-Pakete innerhalb eines definierten Zeitraums reagiert. Der Monitor kann auch Paketverlust und Roundtrip-Dauer während des Tests berechnen. Der Monitor löst nur bei einer Paketverluststufe aus, wenn die Roundtrip-Dauer innerhalb des angegebenen Rahmens liegt.

> **Hinweis:** Das Ping-Protokoll ist eines der Protokolle mit der niedrigsten Priorität in einem Netzwerk und manche Hosts reagieren standardmäßig nicht auf Ping-Pakete.

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Zeitlimit** – Die längste Roundtrip-Dauer in Millisekunden, die der Monitor auf die Rückkehr des Ping-Pakets vom Host wartet.
- **Paketverlust** – Maximaler Paketverlust bei Übertragung an den Host. Wird in Prozent der Gesamtzahl gesendeter Pakete angegeben.
- **Zu sendende Pakete** – Die Anzahl der Pakete, die bei jedem Test gesendet werden. Ein höherer Wert ergibt einen genaueren Wert für den Paketverlust und die Roundtrip-Dauer.
- **Ablaufverfolgung einschließen** – Wählen Sie eine Option aus, um bei Alarmmeldungen ein Traceroute-Protokoll einzuschließen.
- **Max. Hops** – Maximale Anzahl der Traceroute-Hops, die im Alarmstatus durchgeführt werden. Standardeinstellungen auf `255`.
- **Alternative IP** – Zu testende sekundäre IP. Der Monitor kann eine alternative IP-Adresse im selben Test pingen.
- **Paketgröße** – Gesamtgröße der mit dem Paket gesendeten Daten. Schließt die IP- und die ICMP-Kopfzeilengröße von 28 Byte aus. Um beispielsweise ein MTU von 1500 zu testen, geben Sie hier 1472 ein.
- **Nicht fragmentieren** – Stellt die Option "Nicht fragmentieren" in den ausgehenden Ping-Paketen ein.

POP3-Servermonitor

Der **POP3-Servermonitor** verbindet sich mit einem POP3-Mailserver und prüft, ob er sich mit dem Server verbinden und diesen auf E-Mails überprüfen kann, ohne den Status des Postfachs zu beeinträchtigen. So wird geprüft, ob die POP3-Authentifizierung und das Speichersystem des POP3-Servers funktionieren. Wenn kein Benutzername oder Kennwort angegeben ist, wird ein einfacher Verbindungstest durchgeführt.

- Systemtyp: Alle
- Kategorie: Internet und E-Mail

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Benutzername/Kennwort** – Optional. Benutzernamen und Kennwort eines POP3-Kontos
- **Port-Nummer** – Die Port-Nummer, für deren Verwendung der POP3-Server konfiguriert ist.

Prozessstatusmonitor

Der **Prozessstatusmonitor** kann überprüfen, ob ein Prozess auf einem Bestand ausgeführt wird.

- Systemtyp: Alle außer Andere/Unbekannt
- Kategorie: Leistung

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Prozessname** – Der Name des zu überwachenden Prozesses.
- **Nicht gelisteter Prozess** – Der Name des zu überwachenden Prozesses, wenn nicht aufgelistet. Üblicherweise ist ein Dienst nicht aufgelistet, wenn er noch nicht gestartet wurde.
- **Funktion umkehren** – Aktivieren Sie diese Option, damit der Monitortest fehlschlägt, wenn der Prozess ausgeführt wird.
- **Anmeldekonto** – Wählen Sie ein Konto aus der Liste aus, um das Standardkonto des Bestands zu überschreiben.

Radius-Monitor

Der **Radius-Servermonitor** testet die Leistung von Radius-Servern. Radius ist ein Netzwerkprotokoll, das für Computer, die eine Verbindung zu einem Netzwerk herstellen möchten, Authentifizierung, Zugriff und Ressourcenerfassung bietet. Radius wird oft verwendet, um Zugriff auf drahtlose Netzwerke zu bieten. Alle Tests werden mithilfe von SNMP-get-Anforderungen durchgeführt. In der Dokumentation Ihres Radius-Servers können Sie erfahren, ob Ihr Radius-Server standardmäßig auf SNMP-Anforderungen reagiert oder ob Sie diese Funktion konfigurieren müssen.

- Der KNM-Host/Gateway muss als Radius-Client mit dem Radius-Server eingerichtet werden und einen gemeinsamen Schlüssel nutzen.
- Für Vergleichsoptionen muss auf dem Radius-Server außerdem ein laufender SNMP-Agent installiert sein.

Hinweis: Der Communityname (SNMP-Version) und Port, der von **Network Monitor** verwendet wird, um eine Verbindung mit einem SNMP-Bestand zu erstellen, wird in der Registerkarte **Authentifizierung** *(siehe 40)* eines Bestandsknotens festgelegt. Der Bestandsknoten kann diese Einstellung von einem übergeordneten Knoten erben. Siehe **Installationscheckliste** *(siehe 4)*

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

Diese Felder sind erforderlich, um eine Verbindung zum Radius-Server herzustellen und konfigurierte Tests durchzuführen.

- **Schlüssel** – Vorher geteiltes gemeinsames Schlüsselwort, das zur Verschlüsselung aller Kennwörter verwendet wird, die an den Radius-Server zwecks Authentifizierung gesendet werden.
- **Anmeldekonto** – Das Anmeldekonto enthält die zu verwendenden Anmeldedaten für die Authentifizierung mit dem Radius-Server.

Systemmonitoroptionen

Jeder Test wird innerhalb einer bestimmten Zeitspanne durchgeführt. Die Zeitspanne wird in Sekunden angegeben.

- **Max. ungültige Auth.anforderung** – Die maximal erlaubte Anzahl von Zugriffsanforderungspaketen, die von einer unbekannten Adresse während der im unten angegebenen Feld definierten Zeitspanne empfangen werden. Der Test schlägt fehl, wenn die Anzahl diesen Wert übersteigt. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.

- **Max. Ressourcenerfassungsanforderungen** – Die Anzahl der Anforderungspakete zur Ressourcenerfassung, die von einer unbekannten Adresse während der im unten angegebenen Feld definierten Zeitspanne empfangen werden. Der Test schlägt fehl, wenn die Anzahl diesen Wert übersteigt. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.
- **Max. Zugriffsablehnung** – Die maximale Anzahl von Paketen mit abgelehntem Zugriff, die während der im unten angegebenen Feld definierten Zeitspanne gesendet wurden. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.

Vergleichsoptionen

Neben den oben genannten Tests kann eine benutzerdefinierte SNMP-get-Anforderung gemacht werden. Das Ergebnis der Anforderung kann mit einem vordefinierten Wert mithilfe eines Vergleichsvorgangs verglichen werden.

- `Radius compare OID` – Eine zur grundlegenden Radius-OID (`.1.2.6.1.2.1.67` oder `.iso.org.dod.internet.mgmt.mib-2.radiusMIB`) relative OID, die bei jedem Test angefordert und mit einem vordefinierten Vergleichswert verglichen werden kann. Lassen Sie dieses Feld leer, um diesen Test nicht durchzuführen.
- `Compare value` – Wert, mit dem das Abfrageergebnis verglichen wird.
- `Value type` – Typ des Werts, der mit dem aus der Datenbank abgerufenen Wert verglichen wird.
- `Operation` – Vorgang zur Bewertung des ausgegebenen Abfrageergebnisses und des zu bestimmenden Vergleichswerts, wenn der Test erfolgreich war oder fehlgeschlagen ist.

Salesforce-Abfragemonitor

Salesforce-Abfrageserver überwacht eine Salesforce-Datenbank. Der Salesforce-Monitor führt eine SQL-Abfrage aus und vergleicht das Ergebnis mit einem vordefinierten Wert.

- Systemtyp: Windows, Linux/UNIX, Sonstige/Unbekannt
- Kategorie: Datenbank

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Registerkarte "Grundlegend"

Eigenschaften des Salesforce-Monitors

- **SQL-Abfrage** – SQL-Abfrage, die ausgeführt wird.

Salesforce-Konto

- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des Bestands vererbt. Wenn dies deaktiviert ist, geben Sie monitorspezifische Anmeldedaten ein.

  > **Hinweis:** Deaktivieren Sie dieses Kontrollkästchen für den Monitor und geben Sie monitorspezifische Anmeldedaten ein.

- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diesen Monitor verwendet werden.
- **Fehler bei fehlenden Zeilen** – Aktivieren Sie diese Option, damit der Monitor den Test nicht besteht, wenn bei der Abfrage keine Zeilen zurückgegeben werden.
- **Datentyp** – `SQL query value` ist die einzige aktuell unterstützte Option.

Schwellenwerteinstellungen

- **Werttyp** – Der Typ des Werts, der mit dem Wert, der von der Salesforce-Datenbank angefragt wird, verglichen wird.
- **Vorgang vergleichen** – Legen Sie fest, wie der angefragte Wert und der verglichene Wert für einen erfolgreichen Test in Beziehung stehen.
- **Vergleichswert** – Wert, mit dem der abgefragte Wert verglichen wird.
- **Zeitperiode** – Wenn dieses Feld leer ist, wird der **Vergleichswert** mit dem abgefragten Wert verglichen. Wenn der Wert **Zeitperiode** in Sekunden eingegeben wird, wird der **Vergleichswert** mit der Differenz von abgefragten Werten zwischen zwei aufeinanderfolgenden Zeitperioden verglichen.

SMTP-Servermonitor

Der **SMTP-Servermonitor** prüft, ob er sich mit einem SMTP-Server verbinden kann und ob der SMTP-Server einen gültigen Rückgabecode zurückgibt.

- Systemtyp: Alle
- Kategorie: Internet und E-Mail

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Port** – Die Port-Nummer, für deren Verwendung der SMTP-Server konfiguriert ist.

SNMP-Monitor

Der **SNMP**-Monitor ist ein dynamisches Werkzeug zur Abfrage mehrerer Bestandsbezeichner (OID) von einem Remote-SNMP-Agent und führt Berechnungen mit den zurückgegebenen Werten aus.

Hinweis: Der Communityname (SNMP-Version) und Port, der von **Network Monitor** verwendet wird, um eine Verbindung mit einem SNMP-Bestand zu erstellen, wird in der Registerkarte **Authentifizierung** *(siehe 40)* eines Bestandsknotens festgelegt. Der Bestandsknoten kann diese Einstellung von einem übergeordneten Knoten erben. Siehe **Installationscheckliste** *(siehe 4)*

- Systemtyp: Alle
- Kategorie: SNMP

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Einstellungen

- **OID1, 2, 3, ...** – Gibt eine Liste von nummerierten OIDs an.
  - Klicken Sie auf **OID hinzufügen** und **OID entfernen**, um OIDs diesem Monitor hinzuzufügen bzw. von diesem zu entfernen.
  - Sie können sowohl einen benannte OID als auch eine OID im Zahlenformat angeben. Wenn Sie eine benannte OID angeben, versucht **Network Monitor** automatisch, die OID im Zahlenformat aufzulösen, wenn das Feld den Fokus verliert. **Network Monitor**verwendet für den Versuch, das Zahlenformat der OID zu finden, die aktuell kompilierten MIBs.

- Die Schaltfläche **[...]** neben dem OID-Feld zeigt einen MIB-Browserdialog an, der verwendet werden kann, um Bestandsbezeichner vom Remote-SNMP-Agent auszuwählen.
- Wenn der MIB-Browser eine OID-Nummer mit `@string` anzeigt, heißt das, dass Sie diesen String als Teil der OID verwenden können. Zum Beispiel kann die OID `.1.3.6.1.2.1.2.2.1.16@Intel(R) PRO/1000 MT Network Connection` in das OID-Feld eingegeben werden, statt die Indexnummer der Netzwerkverbindung anzugeben.

- **Berechnung** – Eine Berechnung, die die von den Bestandsbezeichnern abgefragten Werte verwendet. Im unten dargestellten Beispiel wird die Netzwerkauslastung von einer Schnittstelle berechnet.
- **Ergebnisübersetzung** – Übersetzt das Ergebnis in einen lesbaren String. Diese Option ist nur verfügbar, wenn der Werttyp im Vergleich auf `string` eingestellt ist. Die Ergebnisübersetzungsfunktion kann verwendet werden, um einen nicht beschreibenden OID-Wert in einen lesbaren String zu übersetzen. Der abgerufene OID-Wert kann immer noch ein numerischer Wert sein, er wird jedoch als String behandelt.

  Beispiel 1

  `Unknown(1), Alarm(2), Failed(3),  Ok(4)`

  Beispiel 2

  `Unknown=1,Alarm=2,Failed=3,OK=4`

  Die Werte 1, 2, 3 und 4 werden in "Unbekannt", "Alarm", "Fehlgeschlagen" und "OK" übersetzt. Beide Beispiele oben sind gültige Notationen. Der endgültige übersetzte String ist der String, der für den Vergleichsvorgang verwendet wird.
- **Gültige Werte / Min. / Max.** – Aktiviert den Monitor, um alle Werte unter- und oberhalb des angegebenen Schwellenwerts herauszufiltern.
- **Datentyp** – Die Dateneinheit, die durch den Test gesammelt wurden. Dadurch ist es möglich, Daten mit anderen Monitoren zu gruppieren, indem derselbe Typ für Berichte verwendet wird.
- **Zählermodus**
  - **Delta** – Berechnet die Differenz zwischen dem letzten Test und dem aktuellen Test. Empfohlen, wenn der zurückgegebene Wert ständig wächst.
  - **Absoluter Wert** – Verwendet den zurückgegebenen absoluten Wert.
- **Werttyp** – Typ des Werts, der mit den abgefragten Daten verglichen wird.
- **Vergleichsvorgang** – Vorgang, der für Vergleiche verwendet wird.
- **Vergleichswert** – Wert, mit dem der Ergebniswert der Berechnung verglichen wird.

SNMP-Trap-Monitor

Der **SNMP-Trap**-Monitor empfängt Trap-Meldungen von SNMP-Monitoren auf Remote-Hosts. Der Monitor empfängt nur Meldungen, die von der IP-Adresse des Bestands stammen. Der erste Filterschritt geschieht mit den angegebenen Unternehmens-OIDs. Eine weitere Untersuchung des Trap geschieht mit dem variablen Bindungsfilter, der mehrere Regeln enthalten kann. Die Regeln werden entweder alle zusammen bewertet ("AND'-Operation) oder nacheinander ("OR'-Operation). Das daraus entstehende Trap löst einen fehlgeschlagenen Test aus. Der Monitor kann die generischen Standard-Trap-Typen SNMP v1 und SNMP v2c herausfiltern.

Jedes OID-Feld kann durch Auswahl aus dem **MIB-Browser** *(siehe 97)* bestückt werden. Der MIB-Browser wird über die Schaltfläche rechts neben dem OID-Feld geöffnet.

Siehe

- Systemtyp: Alle
- Kategorie: SNMP

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Registerkarte "Grundlegend"

- **OID-Einschlussfilter** – Geben Sie eine oder mehrere OIDs mit einem Komma getrennt ein. Der Monitor löst einen Alarm für die angegebene Unternehmens-OID aus.
  - Sie können sowohl einen benannte OID als auch eine OID im Zahlenformat angeben. Wenn Sie eine benannte OID angeben, versucht **Network Monitor** automatisch, die OID im Zahlenformat aufzulösen, wenn das Feld den Fokus verliert. **Network Monitor**verwendet für den Versuch, das Zahlenformat der OID zu finden, die aktuell kompilierten MIBs.
  - Die Schaltfläche **[...]** neben dem OID-Feld zeigt einen MIB-Browserdialog an, der verwendet werden kann, um Bestandsbezeichner vom Remote-SNMP-Agent auszuwählen.
  - Wenn der MIB-Browser eine OID-Nummer mit `@string` anzeigt, heißt das, dass Sie diesen String als Teil der OID verwenden können. Zum Beispiel kann die OID `.1.3.6.1.2.1.2.2.1.16@Intel(R) PRO/1000 MT Network Connection` in das OID-Feld eingegeben werden, statt die Indexnummer der Netzwerkverbindung anzugeben.
- **OID-Ausschlussfilter** – Geben Sie eine oder mehrere OIDs mit einem Komma getrennt ein. Dieser Monitor ignoriert Traps von der angegebenen Unternehmens-OID.
- **Community** – Zu verwendende SNMP-Community.

Registerkarte "Variablenbindungsfilter"

- **Alle Variablen einschließen** – Bei Markierung werden alle Variablenbindungen vom Trap in der Alarmmeldung eingeschlossen. Ist dieses Feld nicht markiert, werden nur *übereinstimmende* Variablenbindungen eingeschlossen.
- **Übereinstimmungsoption** – Wenn `All`, müssen alle Variablenbindungen übereinstimmen. Wenn `At least one`, muss nur eine Variablenbindung übereinstimmen.
- **OID/Wertpaare** – Filterregeln zur Bewertung von Trap-Daten. Führt einen Vergleichsvorgang bei einer dynamischen Anzahl von OIDs im Trap durch. Die Filterregeln können zusammen oder nacheinander bewertet werden. Das Ergebnis des Vorgangs muss mit `true` bewertet werden, damit es als übereinstimmender Trap gilt.

Registerkarte "Trap-Typfilter"

- **Trap-Typfilter** – Trap-Typen, die im Test eingeschlossen werden sollen.

```
Coldstart
Warmstart
Link down
Link up
Authentication failed
EGP
Enterprise
```

SQL Server-Monitor

Der **SQL Server**-Monitortyp kann mehrere wichtige Aspekte einer Microsoft SQL Server-Datenbank überwachen. Der Monitor verwendet die native SQL Server-Schnittstelle und es muss kein ODBC-Treiber auf dem **Network Monitor**-Hostrechner installiert werden.

- Systemtyp: Fenster
- Kategorie: Datenbank

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Registerkarte "Grundlegend"

Grundlegende Monitoreinstellungen

Diese Felder sind erforderlich, um eine Verbindung zur Datenbank herzustellen und konfigurierte Tests durchzuführen.

- **Anmeldekonto** – Das Anmeldekonto enthält die zu verwendenden Anmeldedaten für die Authentifizierung mit der SQL Server-Datenbank.
- **Instanzname** – Der zu verwendende SQL Server-Instanzname.
- **Datenbankname** – Name der Datenbank, zu der eine Verbindung hergestellt wird.
- **Port** – Die Port-Nummer, die der Datenbankserver überwacht. Standardeinstellungen auf Port `1433`.
- **Protokolltyp** – `Default protocol`, `TCP/IP`, `Named Pipes`, `Shared Memory`
- **Datentyp** – `SQL query value`. Dies ist die einzige aktuell unterstützte Option.

Systemmonitoring

> **Hinweis:** Lassen Sie diese Felder leer, um keine Tests durchzuführen.

- **Max. Benutzer** – Max. Anzahl der Benutzer, die gleichzeitig angemeldet sein dürfen.
- **Puffer-Cache-Trefferverhältnis** – Das Puffer-Cache-Trefferverhältnis gibt den Prozentsatz von der Gesamtzahl an Anfragen an, die ohne Zugriff auf den Datenträger bedient wurden. Ein höherer Wert bedeutet eine bessere Datenbankleistung. Stellen Sie diesen Wert auf den niedrigsten akzeptablen Wert ein. Wenn die Quote unter diesen Wert fällt, schlägt der Monitortest fehl.
- **Max. Replikationslatenz** – Ein Wert in Sekunden, der die maximale Zeitdifferenz zwischen Master und Slave wiedergibt. Wird diese Dauer überschritten, schlägt der Monitortest fehl.
- **SQL-Kompilierungen** – Ein numerischer Wert, der die maximale Anzahl erlaubter SQL-Kompilierungen pro Sekunde angibt. Wird dieser Wert überschritten, schlägt der Monitortest fehl. Ein hoher Wert für die SQL-Kompilierungen pro Sekunde kann zu einer hohen CPU-Auslastung führen.

Optionen der Tabellenbereichsüberwachung

> **Hinweis:** Lassen Sie diese Felder leer, um keine Tests durchzuführen.

Ein Tabellenbereich ist mit physikalischen Dateien verknüpft, die auf einer Disk gespeichert sind. Jede Datenbank kann mit einem oder mehreren Tabellenbereichen zur Speicherung von Tabellen und Indizes verknüpft werden. Durch Überwachung der Tabellenbereichsnutzung können Sie gewarnt werden, bevor der verbleibenden Speicherplatz in einem Tabellenbereich einen Schwellenwert unterschreitet.

- **Datenbank-Disknutzung** – Ein Schwellenwert, der die maximal erlaubte Nutzung eines Tabellenbereichs in Prozent angibt. Dieses Feld gilt für alle Tabellenbereiche in der Datenbank, nachfolgende Felder können verwendet werden, um Ausnahmen für diese Regel zu konfigurieren, für bis zu fünf andere Tabellenbereiche.
- **Tabellenbereichsnutzung / % max. Nutzung** (1-5) – Ein Schwellenwert für die maximal erlaubte Nutzung eines bestimmten Tabellenbereichs. Diese Felder überschreiben den globalen Tabellenbereichs-Schwellenwert.

Schwellenwerteinstellungen

Eine optionale SQL-Anweisung kann ausgeführt und ihre Ausgabe mit einem vordefinierten Wert mithilfe einer Vergleichsoperation verglichen werden.

- **SQL-Abfrage** – Optionale SQL-Abfrage, die ausgeführt wird.

- **Fehler bei fehlenden Zeilen** – Aktivieren Sie diese Option, damit der Monitor den Test nicht besteht, wenn bei der Abfrage keine Zeilen zurückgegeben werden.
- **Werttyp** – Typ des Werts, der mit dem aus der Datenbank abgerufenen Wert verglichen werden soll.
- **Vergleichsvorgang** – Vorgang zur Bewertung des ausgegebenen Abfrageergebnisses und des zu bestimmenden Vergleichswerts, wenn der Test erfolgreich war oder fehlgeschlagen ist.
- **Vergleichswert** – Wert, mit dem das Abfrageergebnis verglichen werden soll.

SQL Server-Konto

- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des Bestands vererbt. Wenn dies deaktiviert ist, geben Sie monitorspezifische Anmeldedaten ein.
- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diesen Monitor verwendet werden.

SSH2-Skriptmonitor

Der **SSH2-Skriptmonitor** kann einen Befehl oder ein Skript auf einem SSH2-Host ausführen und den zurückgegebenen Wert mit einem vordefinierten String mithilfe eines Vergleichstyps vergleichen. Wenn der Vergleichsvorgang `false` ergibt, erzeugt der Monitor einen Alarm.

- Systemtyp: Alle
- Kategorie: Skript

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Befehl** – Ein Befehl zur Ausführung auf dem Host. Der Befehl sollte nach der Ausführung einen Wert zurückgeben.
- **Anmeldekonto** – Wählen Sie ein Konto aus der Liste aus, um das Standardkonto des Bestands zu überschreiben.
- **Datentyp** – Die Dateneinheit, die vom Skript zurückgegeben wird. Dadurch ist es möglich, Daten dieses Monitortyps mit anderen Monitoren wie `CPU utilization` in Berichten zu gruppieren.
- **Port** – Port-Nummer
- **Vergleichswert** – Wert, mit dem das zurückgegebene Ergebnis verglichen wird.
- **Werttyp** – Typ des zurückgegebenen Werts.
- **Vorgang** – Vergleichsvorgang, der bei der Bewertung des Ergebnisses verwendet wird. Wenn der zurückgegebene Wert im Vergleich zum Vergleichswert `false` ergibt, schlägt der Monitortest fehl.

SSH2-Servermonitor

Der **SSH2-Servermonitor** überprüft, ob ein SSH2-Server auf Anmeldeversuche von Benutzern reagiert. Dieser Monitor unterstützt nicht das ältere SSH1.x-Protokoll. Wenn keine Anmeldedaten angegeben werden, führt der Monitor nur einen Verbindungstest durch.

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Anmeldekonto** – Wählen Sie ein Konto aus der Liste aus, um das Standardkonto des Bestands zu überschreiben.
- **Port** – Port-Nummer, die der Server überwacht. Standardeinstellungen auf `22`.

Auslagerungsdateiauslastungs-Monitor

Auslagerungsdateiauslastungs-Monitore tauschen die Speicherplatzauslastung im Bestand.

- Systemtyp: Alle außer Andere/Unbekannt
- Kategorie: Leistung

Bei Windows-Beständen sind die Methoden zur Auslagerungsdateiauslastung *WMI* oder *Windows-Leistungsindikatoren*.

- Für WMI oder Windows-Leistungsindikatoren ist ein Windows-Benutzer erforderlich, der Leseberechtigungen für die Registrierung des überwachten Bestands hat.
- Bei der Verwendung von Windows-Leistungsindikatoren muss der Dienst "Remoteregistrierung" aktiviert und auf dem überwachten Bestand gestartet sein.

Bei Unix-Beständen stellt KNM mit SSH2 eine Verbindung zu einem überwachten Bestand her und erzeugt Befehle, die für das ausgewählte Betriebssystem spezifisch sind. Stellen Sie sicher, dass der für UNIX-Bestände verwendete Benutzer erforderliche Befehle bearbeiten kann. `free -m`ist der Standardbefehl. Es kann eine Softwareinstallation auf Ihrem Bestand erforderlich sein.

> **Hinweis:** Wenn Sie Schwierigkeiten mit dem Monitortyp bei Windows-Rechnern haben, versuchen Sie diese durch Deaktivieren des Kontrollkästchens **WMI verwenden** in der **Registerkarte "Erweitert"** *(siehe 50)* des Bestandsknotens zu lösen.
>
> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Max. Auslagerungsauslastung** – Gibt den maximalen Prozentsatz als Schwellenwert an.
- **Auslagerungsdateiname** – Der Name der zu überwachenden Auslagerungsdatei. Klicken Sie auf die Verknüpfung **Auslagerungsdateien neu scannen**, um die Liste zu aktualisieren.
- **Anmeldekonto** – Wählen Sie ein Konto aus der Liste aus, um das Standardkonto des Bestands zu überschreiben.

Windows-spezifische Eigenschaften

- **Detaillierter Fehlerbericht** – Listet alle Prozesse und ihre Speichernutzung in einem Fehlerbericht auf.

Syslog-Monitor

Der **Syslog**-Monitor kann eine Syslog-Meldung abfangen, die von einem oder mehreren Syslog-Hosts an **Network Monitor** gesendet wurde. Der Monitor kann so konfiguriert werden, dass er verschiedene Meldungstypen empfängt. Jedem Bestand kann mehr als ein Syslog-Monitor hinzugefügt werden, um verschiedene Meldungskombinationen zu empfangen.

- Systemtyp: Alle
- Kategorie: Protokoll

Voraussetzungen

- Aktivieren Sie die Sammlung von Syslog-Meldungen einzeln für jedes Gateway, indem Sie das Kontrollkästchen Network Monitor > (ausgewähltes Gateway) > Bearbeiten > **Registerkarte "Erweitert"** *(siehe 38)* > **Syslog-Server** markieren.
- Zeigen Sie die abgefangenen Syslog-Meldungen auf der Seite Network Monitor Werkzeuge > **Syslog-Meldungen auflisten** *(siehe 101)* an.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **String(s) einschließen** – Filtert Meldungen heraus, die diese Strings nicht enthalten. Trennen Sie mehrere Strings mit einem Komma.
- **String(s) ausschließen** – Meldung wird nicht eingeschlossen, wenn sie nicht einen der in diesem Feld angegebenen Strings enthält. Trennen Sie mehrere Strings mit einem Komma.

TCP-Port-Scan-Monitor

Der **TCP-Port-Scan**-Monitor prüft, ob die angegebenen Ports entweder offen oder geschlossen sind. Standardmäßig wird ein Alarm ausgelöst, wenn die angegebenen Ports offen sind. Wenn die **Umkehrfunktion** markiert ist, wird ein Alarm ausgelöst, wenn die angegebenen Ports geschlossen sind.

- Systemtyp: Alle
- Kategorie: Andere

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Port-Nummerbereich** – Löst einen Alarm aus, wenn die angegebenen Ports offen sind. Portbereiche verwenden das folgende Format:
  - `21-23` – Der Monitor scannt Ports zwischen 21 und 23 (beide einschließlich).
  - `80,21-23` – Der Monitor scannt Port 80 und Ports zwischen 21 und 23 (beide einschließlich). Der Monitor kann bis zu 100 Ports prüfen.
- **Funktion umkehren** – Bei Markierung wird ein Alarm ausgelöst, wenn die angegebenen Ports geschlossen sind.

Telnet-Servermonitor

Der **Telnet-Servermonitor** überprüft, ob ein Telnet-Server reagiert.

- Systemtyp: Alle
- Kategorie: Netzwerkdienst

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Port** – Die Port-Nummer, für deren Verwendung der Telnet-Server konfiguriert ist. Standardeinstellungen auf `23`.

Terminaldienstmonitor

Der **Terminaldienstmonitor** reagiert auf neue Anmeldesitzungen.

- Systemtyp: Alle außer Andere/Unbekannt
- Kategorie: Netzwerkdienste

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Port** – Die Port-Nummer, für deren Verwendung der Terminal-Server konfiguriert ist. Standardeinstellungen auf `3389`.

TFTP-Servermonitor

Der **TFTP-Servermonitor** testet, ob ein TFTP-Server auf einen RRQ-Vorgang reagiert. Zweck dieses Tests ist zu überprüfen, ob der TFTP-Server ausgeführt wird. Der Monitor versucht, eine Datei namens `KNM` herunterzuladen. Diese Datei muss nicht vorhanden sein, damit der Test Erfolg hat. Der Monitor überprüft vielmehr einfach, ob der TFTP-Server korrekt auf eine solche Anfrage reagiert.

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Port** – Die Port-Nummer, für deren Verwendung der TFTP-Server konfiguriert ist. Standardeinstellungen auf `69`.

Übertragungsgeschwindigkeitsmonitor

Der **Übertragungsgeschwindigkeitsmonitor** misst die Übertragungsgeschwindigkeit zwischen **Network Monitor** und einem Bestand. Der Test misst die Zeit, die zum Herunterladen der angegebenen Datenmenge vom `chargen.exe`-Server nötig ist, welcher auf dem Bestand läuft.

Ein `chargen` (Character Generator)-Server muss auf dem Bestand installiert sein und ausgeführt werden. Microsoft stellt einen `chargen`-Server für Windows als Teil des Dienstes **Einfache TCP/IP-Dienste** zur Verfügung. Dieser Dienst ist üblicherweise als Funktion auf Windows-Servern installiert. Der `chargen.exe`-Server verwendet standardmäßig Port 19 (TCP).

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

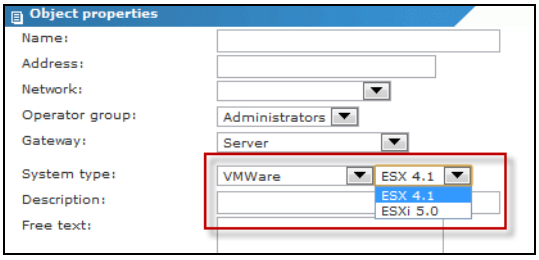
- **Übertragungsgeschwindigkeit** – Mindestübertragungsgeschwindigkeit in der ausgewählten Einheit.
- **Einheit** – Die Einheit, in der der Übertragungsgeschwindigkeitstest aufgezeichnet wird. Wird in Echtzeitgrafiken und Berichten angezeigt.
- **Datengröße** – Größe, in Kilobyte, der gesamten Datenmenge, die im Test empfangen wird.
- **Port-Nummer** – Die Port-Nummer, für deren Verwendung der TFTP-Server konfiguriert ist. Standardeinstellungen auf `19`.

VMware-Systemmonitor

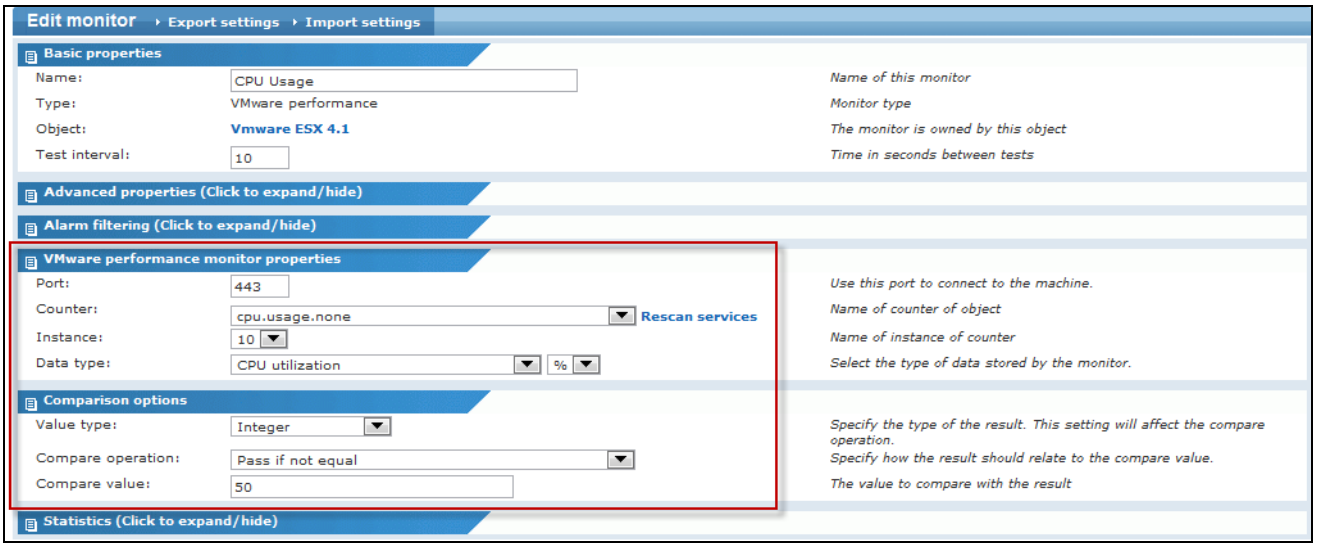
Der **VMware-Systemmonitor** kann einen VMWare-Leistungsindikator für einen VMware-Host oder einen vCenter-Server abfragen und diesen im Rahmen eines Vergleichsvorgangs mit einem bestimmten Wert vergleichen. Wenn der Vergleichsvorgang `false` ergibt, schlägt der Monitortest fehl. Unterstützt ESX 4.1 & ESXi 5. Nimmt keine Änderungen am Ziel-VMware-Hostrechner vor. Unterstützt werden die meisten Leistungsindikatorbestände, wie z. B. Hosts, Datenspeicher und virtueller Speicher. VMware-Zähler für Gäste (virtuelle Maschinen) werden nicht unterstützt.

- Systemtyp: VMware
- Kategorie: Leistung

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.



Identifizieren Sie den Bestand als einen VMware-Systemtyp


Edit monitor
Export settings
Import settings
Basic properties
Name: CPU Usage — Name of this monitor
Type: VMware performance — Monitor type
Object: Vmware ESX 4.1 — The monitor is owned by this object
Test interval: 10 — Time in seconds between tests
Advanced properties (Click to expand/hide)
Alarm filtering (Click to expand/hide)
VMware performance monitor properties
Port: 443 — Use this port to connect to the machine.
Counter: cpu.usage.none Rescan services — Name of counter of object
Instance: 10 — Name of instance of counter
Data type: CPU utilization % — Select the type of data stored by the monitor.
Comparison options
Value type: Integer — Specify the type of the result. This setting will affect the compare operation.
Compare operation: Pass if not equal — Specify how the result should relate to the compare value.
Compare value: 50 — The value to compare with the result
Statistics (Click to expand/hide)

Die Seite "VMware-Systemmonitoreigenschaften"

Monitorspezifische Eigenschaften

- **Zähler/Instanz** – Name des primären zu testenden Leistungsindikators. Das Instanzfeld ist absichtlich bei manchen Zählertypen leer gelassen. Ein Scan zählt automatisch die angezeigten Werte auf. Klicken Sie auf die Verknüpfung **Neu scannen**, um diese Werte zu aktualisieren.
- **Datentyp** – Die Einheit der Daten, die im Rahmen des Tests aufgezeichnet werden. Dadurch ist es möglich, Daten dieses Monitortyps mit anderen Monitoren wie `CPU utilization` in Berichten zu gruppieren.
- **Werttyp** – Typ des ausgegebenen Werts.
- **Vergleichsvorgang** – Vorgang zur Bewertung des ausgegebenen Ergebnisses und des vordefinierten Vergleichswerts.
- **Vergleichswert** – Benutzerdefinierter Vergleichswert. Es sind nur numerische Werte zulässig.

Webservermonitor

Der **Webservermonitor** kann einen Webserver testen und den Inhalt der angeforderten Seite überprüfen. Stellen Sie sicher, dass der Inhalt der angeforderten Seite seit dem letzten Test nicht geändert wurde. Suchen Sie nach einem String auf der Seite und überprüfen Sie Verknüpfungen.

- Systemtyp: Alle
- Kategorie: Netzwerkdienste

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Registerkarte "Grundlegend"

URL- & Anforderungseinstellungen

- **URL** – Die URL der herunterzuladenden Seite, relativ zur Webserveradresse. Die angegebene URL legt die Verknüpfung fest, die im Verknüpfungsbereich auf der Webservermonitor-Seite angezeigt wird.
- **Sicheres HTTP verwenden** – Markieren Sie diese Option, damit der Monitor über sicheres HTTP (SSL) kommuniziert.
- **Port** – Port-Nummer, mit der eine Verbindung zum Webserver hergestellt wird.

Schwellenwerteinstellungen

- **Suchstring** – Der String, nach dem die Seite sucht. Wird er nicht gefunden, so schlägt der Test fehl.
- **Seitenabrufzeit** – Ein Schwellenwert in Millisekunden. Wenn die Seite nicht innerhalb dieses Werts geliefert wird, schlägt der Test fehl.
- **Prüfsumme prüfen** – Prüfoption, damit der Monitor den Prüfsummenwert der Seite berechnet. Wenn sich der Prüfsummenwert zwischen zwei Tests ändert, schlägt der aktuelle Test fehl. *Um die Prüfsumme zurückzusetzen, öffnen Sie die Seite "Eigenschaften" und speichern Sie den Monitor.*
- **Login durchführen** – Bei Markierung wird der HTTP-Kontobereich unten angezeigt. Meldet sich beim Server mit den angegebenen Anmeldedaten an.

HTTP-Konto

- **Anmeldedaten erben** – Ist diese Option aktiviert, werden die Anmeldedaten des Bestands vererbt. Wenn dies deaktiviert ist, geben Sie monitorspezifische Anmeldedaten ein.

- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diesen Monitor verwendet werden.
- **Port** – Der Port, der genutzt wird, um eine Verbindung zum HTTP-Konto herzustellen.

Registerkarte "Erweitert"

Erweiterte Einstellungen des Webservermonitors

- **Benutzer-Agent** – Überschreibt die Variable für den Standard-Benutzer-Agent, die in der Anforderung gesendet wird.
- **Benutzerdefiniertes Cookie** – Optionales Cookie, das mit der "get'-Anforderung gesendet wird.
- **Benutzerdefinierter Host** – Optionale Hostkopfzeile, um benannte virtuelle Basishosts zu unterstützen.
- **CN-Prüfung ignorieren** – Bei Markierung prüft der Monitor nicht den allgemeinen Namen des Serverzertifikats. Diese Option ist nur gültig, wenn der Monitor sicheres HTTP verwendet.
- **Datenprüfung ignorieren** – Bei Markierung prüft der Monitor nicht das Ablaufdatum des Serverzertifikats. Diese Option ist nur gültig, wenn der Monitor sicheres HTTP verwendet.
- **CA-Prüfung ignorieren** – Bei Markierung prüft der Monitor nicht die Zertifizierungsstelle des Serverzertifikats. Diese Option ist nur gültig, wenn der Monitor sicheres HTTP verwendet.
- **Zertifikatsspeicher** – Name des Systemzertifikatsspeichers. Verwenden Sie dies nur, wenn der Monitor ein Client-Zertifikat an den Server senden soll.
- **Zertifikatantragsteller** – Betreffzeile des Zertifikats, die im Systemzertifikatsspeicher verwendet werden soll. Verwenden Sie dies nur, wenn der Monitor ein Client-Zertifikat an den Server senden soll.
- **Proxy-Server** – Optionale Adresse des Proxy-Servers.
- **Proxy-Port** – Optionaler Serverport des Proxy-Servers.

Windows-Systemmonitor

Der **Windows-Systemmonitor**kann einen Windows-Leistungsindikator abfragen, um ihn mit einem Vergleichswert mithilfe eines Vergleichsvorgangs zu vergleichen. Wenn der Vergleichsvorgang `false` ergibt, schlägt der Monitortest fehl. Optional können zwei Leistungsindikatoren abgefragt und kombiniert werden, bevor sie mit dem Vergleichswert verglichen werden.

- Systemtyp: Fenster
- Kategorie: Leistung

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Objekt/Zähler/Instanz** – Name des primären zu testenden Leistungsbestands. Diese Werte können mithilfe der Aufzählungsfunktion aufgezählt werden. Das Instanzfeld ist absichtlich bei manchen Zählertypen leer gelassen. Klicken Sie auf die Verknüpfung **Neu scannen**, um diese Werte zu aktualisieren.
- **Objekt/Zähler/Instanz** – Optional. Sekundärer Leistungsbestand. Diese Werte können mithilfe der Aufzählungsfunktion aufgezählt werden. Das Instanzfeld ist absichtlich bei manchen Zählertypen leer gelassen.
- **Kombinationsvorgang** – Optionaler Vorgang, der bei Abfrage von zwei Zählern verwendet wird. Sie können mit dem Additions-, Subtraktions-, Divisions- oder Multiplikationsvorgang zu einem Endergebnis kombiniert werden.
- **Divisor** – Ein Wert, durch den der erhaltene Wert vor dem Vergleich dividiert wird.

- **Datentyp** – Die Dateneinheit, die durch den Test gesammelt wurden. Dadurch ist es möglich, Daten mit anderen Monitoren zu gruppieren, indem derselbe Typ für Berichte verwendet wird.
- **Werttyp** – Typ des Werts, der mit den abgefragten Daten verglichen wird.
- **Vergleichsvorgang** – Vorgang, der für Vergleiche verwendet wird.
- **Vergleichswert** – Wert, mit dem der Ergebniswert der Berechnung verglichen wird.
- **Anmeldedaten erben** – Legt die Anmeldedaten für die Windows-Domäne fest, falls erforderlich. Bei Markierung werden diese vererbt. Wenn dies deaktiviert ist, werden die Anmeldedaten für die Windows-Domäne, die in der Registerkarte **Authentifizierung** *(siehe 40)* für den Bestand festgelegt wurden, überschrieben.

Windows-Dienststatusmonitor

Der **Windows-Dienststatusmonitor** testet, ob ein Windows-Dienst ausgeführt wird.

- Systemtyp: Fenster
- Kategorie: Leistung

Hinweis: An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Verfügbare Dienste** – Liste der Dienste, aus denen ausgewählt werden kann. Klicken Sie auf die Schaltfläche **Auswählen**, um den ausgewählten Dienst an das Feld "Dienstname" anzuhängen. Um die Liste zu aktualisieren, klicken Sie auf die Verknüpfung **Dienste erneut suchen**.
- **Dienstname** – Der Name des zu überwachenden Dienstes. Trennen Sie mehrere Dienste mit einem Komma. Wenn Sie diesen Monitor mit einer **Windows-Dienststeuerungsaktion** *(siehe 163)* kombinieren, kann nur ein Dienst ausgewählt werden.
- **Funktion umkehren** – Bei Markierung löst der Monitor einen Alarm aus, wenn einer der aufgelisteten Dienste ausgeführt wird.
- **Anmeldedaten erben** – Legt die Anmeldedaten für die Windows-Domäne fest, falls erforderlich. Bei Markierung werden diese vererbt. Wenn dies deaktiviert ist, werden die Anmeldedaten für die Windows-Domäne, die in der Registerkarte **Authentifizierung** *(siehe 40)* für den Bestand festgelegt wurden, überschrieben.

Weitere Informationen siehe auch:

- **Windows-Dienststeuerung** *(siehe 172)* (geplantes Ereignis)
- **Windows-Dienststeuerung** *(siehe 163)* (Aktion)
- **Liste der Windows-Dienste** *(siehe 96)* (direkte Steuerung)

WMI-Abfragemonitor

Der **WMI-Abfragemonitor** kann verwendet werden, um WQL-Abfragen auszuführen und bedingte Tests am zurückgegebenen Wert durchzuführen. Der Monitor kann alle Standard-WQL-Abfragen ausführen, aber der Vergleich des zurückgegebenen Werts ist auf ein Feld der zurückgegebenen Daten beschränkt.

- Systemtyp: Fenster
- Kategorie: Leistung

Hinweis: Siehe **Windows-Verwaltungsinstrumentation** *(siehe 195)*.

> **Hinweis:** An dieser Stelle sind nur monitorspezifische Einstellungen dokumentiert. Siehe **Monitorstandardeinstellungen** *(siehe 63)*.

Monitorspezifische Eigenschaften

- **Namespace** – Namespace, innerhalb dessen die Abfrage ausgeführt wird. Der Standard-Namespace lautet `root\cimv2`.
- **WQL** – Eine WQL-Abfrage.
- **Wertname** – Der Name des abzurufenden Werts, wenn die Abfrage ausgeführt wurde. Wenn mehr als eine Ergebniszeile zurückgegeben wird, wird der Wert aus der ersten Zeile des Ergebnisses abgerufen.
- **Datentyp** – Die Dateneinheit, die durch den Test gesammelt wurden. Dadurch ist es möglich, Daten mit anderen Monitoren zu gruppieren, indem derselbe Typ für Berichte verwendet wird.
- **Werttyp** – Typ des Werts, der mit den abgefragten Daten verglichen wird.
- **Vergleichsvorgang** – Vorgang, der für Vergleiche verwendet wird.
- **Vergleichswert** – Wert, mit dem der Ergebniswert der Berechnung verglichen wird.

Kapitel 4

Aktionsreferenz

Dieses Kapitel enthält eine Referenz für alle verfügbaren Aktionen und deren zugehörige Einstellungen. Aktionen werden in der **Registerkarte "Aktionen"** *(siehe 56)* verwendet.

In diesem Kapitel

Aktion "Ereignisprotokoll löschen" 156
Aktion "Befehl über SSH2 ausführen" 156
Aktion "Windows-Befehl ausführen" 157
Aktion "HTTP Get/Post" 157
Aktion "Liste zurücksetzen" 158
Aktion "Lua-Skript" 159
Aktion "E-Mail senden" 159
Aktion "Nachricht über PageGate senden" 160
Aktion "SMS senden" 160
Aktion "Wake-On-LAN-Paket senden" 161
Aktion "SNMP-Set" 161
Ticket-Aktion 162
Aktion "Windows-Dienststeuerung" 163

Aktion "Ereignisprotokoll löschen"

Die Aktion **Ereignisprotokoll löschen** löscht ein Ereignisprotokoll auf einem angegebenen Windows-Host.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Verbinden mit** – `Monitor host` oder `Specific host`. Füllen Sie **Hostname** aus, wenn es einen bestimmten Host gibt.
- **Hostname** – Der Hostname oder die IP-Nummer. Füllen Sie das Feld nicht aus, wenn Sie die Adresse des Bestands verwenden möchten.
- **Anmeldedaten** – `Monitor credentials` oder `Stored credentials`.
- **Anmeldedaten erben** – Wenn gespeicherte Anmeldedaten ausgewählt wurden, wird die Option **Anmeldedaten erben** angezeigt. Bei Markierung werden Anmeldedaten des Bestands vererbt. Geben Sie vorgangsspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diese Aktion verwendet werden.
- **Protokollname** – Name des zu löschenden Protokolls. Zum Beispiel `Application`.

Aktion "Befehl über SSH2 ausführen"

Die SSH2-Aktion führt einen Befehl auf einem SSH2-Server aus. Optional kann die Aktion so konfiguriert werden, dass sie stattdessen das Telnet-Protokoll verwendet.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Verbinden mit** – `Monitor host` oder `Specific host`. Füllen Sie **Hostname** aus, wenn es einen bestimmten Host gibt.
- **Hostname** – Der Hostname oder die IP-Nummer. Füllen Sie das Feld nicht aus, wenn Sie die Adresse des Bestands verwenden möchten.
- **Verbindungstyp** – `SSH` oder `Telnet`. Wenn Telnet gilt, stellen Sie mithilfe der Registerkarte Network MonitorEinstellungen> **Andere Systemeinstellungen** *(siehe 109)* > **Monitorstandardeinstellungen** sicher, dass die Telnet-Parameter richtig konfiguriert sind.

Warnung: Denken Sie daran, dass Telnet nicht verschlüsselt ist und Benutzername/Kennwort in Klartext gesendet werden.

- **Befehl** – Auszuführender Befehl. Die folgenden Formatierungsvariablen können bei der Angabe eines Befehls eingeschlossen werden.
  - `%[asset.name]` – Bestandsname
  - `%[monitor.name]` – Monitorname
  - `%[asset.ip]` – Bestandsadresse
- **Port-Nummer** – Die Port-Nummer, die der SSH2-Server überwacht.
- **Anmeldedaten** – `Monitor credentials` oder `Stored credentials`.
- **Anmeldedaten erben** – Wenn gespeicherte Anmeldedaten ausgewählt wurden, wird die Option **Anmeldedaten erben** angezeigt. Bei Markierung werden Anmeldedaten des Bestands vererbt. Geben Sie vorgangsspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diese Aktion verwendet werden.

Aktion "Windows-Befehl ausführen"

Die Aktion **Windows-Befehl ausführen** führt einen Befehl auf dem **Network Monitor**-Hostrechner aus. Der Befehl wird als Systembenutzerprozess ausgeführt und kann keine Interaktion mit dem Benutzer anfordern.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Befehl** – Auszuführender Befehl. Der Befehl ist eine ausführbare Datei, die sich im KNM-Stammverzeichnis oder im Windows- oder System32-Verzeichnis befindet.
- **Parameter** – Ein String, der an den ausgeführten Befehl als Argumente geleitet wird.
- **Anmeldedaten** – `Monitor credentials` oder `Stored credentials`.
- **Anmeldedaten erben** – Wenn gespeicherte Anmeldedaten ausgewählt wurden, wird die Option **Anmeldedaten erben** angezeigt. Bei Markierung werden Anmeldedaten des Bestands vererbt. Geben Sie vorgangsspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diese Aktion verwendet werden.

Aktion "HTTP Get/Post"

Die Aktion **HTTP Get/Post** sendet die Anforderung "HTTP Get" oder "Post" an einen Webserver.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Verbinden mit** – `Monitor host` oder `Specific host`. Füllen Sie **Hostname** aus, wenn es einen bestimmten Host gibt.
- **Hostname** – Der Hostname oder die IP-Nummer. Füllen Sie das Feld nicht aus, wenn Sie die Adresse des Bestands verwenden möchten.
- **Get/Post** – Methode beim Versenden der Anforderung an den Webserver.
- **URL** – Die URL kann absolut oder relativ zum Bestand sein.
- **SSL** – Markieren Sie die Option, um SSL zu verwenden. Beachten Sie, dass der Webserver normalerweise einen anderen Port als den Standardport 80 für SSL-Datenverkehr überwacht. Ändern Sie bei Bedarf die Port-Nummer bei Auswahl dieser Option. Die Aktion akzeptiert Zertifikate von Serverseite mit einem ungültigen allgemeinen Namen, einem abgelaufenen Datum oder einer ungültigen Zertifizierungsstelle. Wird dieses Kontrollkästchen markiert bzw. die Markierung daraus entfernt, so wechselt die Port-Nummer zwischen 80 (nicht markiert) und 443 (markiert).
- **Port** – Port-Nummer Standardeinstellungen auf `80`.
- **Parameter** – *Nur bei POST-Anfragen.* Geben Sie Parameter im Format `name=value` ein, ein Parameter pro Zeile. Die folgenden **Formatierungsvariablen** *(siehe 66)* können bei einem Parameter eingeschlossen werden.
  - `%[system.time]` – aktuelle Zeit
  - `%[asset.name]` – Bestandsname
  - `%[asset.address]` – Bestandsadresse
  - `%[monitor.name]` – Monitorname
  - `%[monitor.error]` – Monitorfehlermeldung
  - `%[monitor.error2]` – Monitorfehlermeldung, kein Zeitstempel
  - `%[asset.description]` – Bestandsbeschreibung
  - `%[group.name]` – Gruppenname

    - `%[group.contact]` – Gruppenkontakt
- **Zeichencodierung** – `ISO-8859-1` oder `UTF-8`. Die von der Anfrage verwendete Codierung.
- **HTTP-Authentifizierung** – Geben Sie, wenn dies markiert ist, Anmeldedaten ein, um die Anfrage zu authentifizieren.
- **Anmeldedaten** – `Monitor credentials` oder `Stored credentials`.
- **Anmeldedaten erben** – Wenn gespeicherte Anmeldedaten ausgewählt wurden, wird die Option **Anmeldedaten erben** angezeigt. Bei Markierung werden Anmeldedaten des Bestands vererbt. Geben Sie vorgangsspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diese Aktion verwendet werden.
- **Proxy-Einstellungen**
    - **Proxy-Server** – Adresse des Proxy-Servers.
    - **Proxy-Port** – Portnummer des Proxy-Servers.

Beispiel: "Get"- und "Post'-Anforderungen mit absoluter URL

Dieses Beispiel zeigt zwei verschiedene Arten, Anforderungen mit Variablen an einen Webserver zu senden, entweder mit der "Get'-Anforderung oder mit der "Post'-Anforderung.

"Get'-Anforderung

- **URL** - `http://www.yourserver.com/test.php?test1=1&test2=2`

"Post'-Anforderung

- **URL** - `http://www.yourserver.com/test.php`
- **Parameter**
    - `test1=1`
    - `test2=2`

Beispiel: "Get"- und "Post'-Anforderungen mit relativer URL

Dieses Beispiel zeigt zwei verschiedene Arten, Anforderungen mit Variablen an einen Webserver zu senden, entweder mit der "Get'-Anforderung oder mit der "Post'-Anforderung. Die URL ist relativ zur Adresse des Bestands, der die Aktion aufruft.

"Get'-Anforderung

- **URL** - `test.php?test1=1&test2=2`

"Post'-Anforderung

- **URL** - `test.php`
- **Parameter**
    - `test1=1`
    - `test2=2`

Aktion "Liste zurücksetzen"

Die Aktion "Liste zurücksetzen" führt bei Ausführung dazu, dass die Ausführung ab der ersten Aktion neu startet. Die Aktion "Liste zurücksetzen" kann verwendet werden, um ein *Schleifenverhalten* hervorzurufen. Die Aktion "Liste zurücksetzen" ist nicht als Wiederherstellungsaktion verfügbar.

Aktion "Lua-Skript"

Die Aktion **Lua-Skript** führt ein **Lua** *(siehe 205)*-Skript aus; der Bestand des Monitors, der die Aktion aufruft, wird vom Skript als Host verwendet. Die Aktion "Lua-Skript" kann sowohl einfache als auch erweiterte Skripte ausführen. Skripte, die das erweiterte Skriptmodell verwenden, haben benutzerdefinierte Argumentenabschnitte, die hier nicht beschrieben sind.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Autor** – Der Verfasser des Lua-Skripts.
- **Version** – Die Version der des Lua-Skripts.
- **Beschreibung** – Eine Zusammenfassung des Lua-Skripts in einer Zeile.

> **Hinweis:** Hier werden zusätzliche Parameter angezeigt, nach Bedarf zur Unterstützung des Lua-Skripts.

- **Anmeldedaten**
  - `No authentication` – Es werden keine anderen Anmeldedateneinstellungen benötigt.
  - `Use specific credentials in API` – Stellen Sie den **Kontotyp** auf `Windows domain account`, `SSH/Telnet account` oder `VMware account` ein.
  - `Perform Windows impersonation` – Verwenden Sie ein Benutzeranmeldekonto.
- **Anmeldedaten erben** – Wenn `Use specific credential in API` oder `Perform Windows impersonation` aktiviert sind, wird die Option **Anmeldedaten erben** angezeigt. Bei Markierung werden Anmeldedaten des Bestands vererbt. Geben Sie vorgangsspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diese Aktion verwendet werden.

Aktion "E-Mail senden"

Die Aktion **E-Mail senden** sendet eine E-Mail an einen oder mehrere Empfänger. Die Nachricht wird in dem Format formatiert, das angegeben oder vom Monitor geerbt wurde.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Diensthabende Benutzer** – Die Nachricht wird nur an diensthabende Benutzer gesendet. Wenn kein Benutzer Dienst hat, wird keine Nachricht gesendet.
- **Benachrichtigungsgruppe** – Die Nachricht wird an alle Benutzer in der Benutzergruppe gesendet, die dem Bestand zugewiesen ist.
- **Gruppenmanager** – Die Nachricht wird nur an den Benutzer gesendet, der als Gruppenmanager der Benutzergruppe ausgewiesen ist, welche dem Bestand zugewiesen ist. Wenn eine Benutzergruppe keinen ausgewiesenen Gruppenmanager hat, wird keine Nachricht gesendet.
- **Bestimmte Benutzergruppe** – Die Nachricht wird an die ausgewählte Benutzergruppe gesendet. Mit dieser Option können Sie den Alarm steigern, sodass er mehr Benutzer als nur die in der Benutzergruppe, die dem Bestand zugewiesen ist, umfasst.
- **Bestimmter Empfänger** – Die Nachricht wird an eine bzw. mehrere durch Semikolon getrennte E-Mail-Adressen gesendet.
- **Kurznachricht** – Bei Markierung wird eine komprimierte Nachricht gesendet. Zum Beispiel, wenn die Nachricht über ein SMS-Gateway gesendet wird. Bei dieser Option werden die folgenden Informationen entfernt, um die Nachrichtengröße zu erhalten:

- `%[asset.description]` – Bestandsbeschreibung
- `%[user.distribution_list]` – Verteilungsliste
- `%[system.charts]` – Echtzeitdiagramme
- `%[monitor.dependency_status]` – Abhängigkeitsstrukturstatus
- `%[monitor.error]` – Monitorfehlermeldung
- `%[network.contact]` – Netzwerkkontakt

Aktion "Nachricht über PageGate senden"

Die Aktion **Nachricht über PageGate senden** sendet eine Nachricht an einen Pagegate-Benutzer. Die Nachricht wird in dem Format formatiert, das angegeben oder vom Monitor geerbt wurde.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Diensthabende Benutzer** – Die Nachricht wird nur an diensthabende Benutzer gesendet. Wenn kein Benutzer Dienst hat, wird keine Nachricht gesendet.
- **Benachrichtigungsgruppe** – Die Nachricht wird an alle Benutzer in der Benutzergruppe gesendet, die dem Bestand zugewiesen ist.
- **Gruppenmanager** – Die Nachricht wird nur an den Benutzer gesendet, der als Gruppenmanager der Benutzergruppe ausgewiesen ist, welche dem Bestand zugewiesen ist. Wenn eine Benutzergruppe keinen ausgewiesenen Gruppenmanager hat, wird keine Nachricht gesendet.
- **Bestimmte Benutzergruppe** – Die Nachricht wird an die ausgewählte Benutzergruppe gesendet. Mit dieser Option können Sie den Alarm steigern, sodass er mehr Benutzer als nur die in der Benutzergruppe, die dem Bestand zugewiesen ist, umfasst.
- **Bestimmter Empfänger** – Die Nachricht wird an eine bzw. mehrere durch Semikolon getrennte E-Mail-Adressen gesendet.
- **Kurznachricht** – Bei Markierung wird eine komprimierte Nachricht gesendet. Zum Beispiel, wenn die Nachricht über ein SMS-Gateway gesendet wird. Bei dieser Option werden die folgenden Informationen entfernt, um die Nachrichtengröße zu erhalten:
  - `%[asset.description]` – Bestandsbeschreibung
  - `%[user.distribution_list]` – Verteilungsliste
  - `%[system.charts]` – Echtzeitdiagramme
  - `%[monitor.dependency_status]` – Abhängigkeitsstrukturstatus
  - `%[monitor.error]` – Monitorfehlermeldung
  - `%[network.contact]` – Netzwerkkontakt

Aktion "SMS senden"

Die Aktion **SMS senden** sendet eine SMS an einen oder mehrere Empfänger. Die Nachricht wird in dem Format formatiert, das angegeben oder vom Monitor geerbt wurde. Die Nachricht darf höchstens 160 Zeichen lang sein. Ein längerer Text wird vor Absenden der SMS abgeschnitten.

Um diese Aktion verwenden zu können, müssen die **SMS-Einstellungen** *(siehe 110)* konfiguriert sein.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Diensthabende Benutzer** – Die Nachricht wird nur an diensthabende Benutzer gesendet. Wenn kein Benutzer Dienst hat, wird keine Nachricht gesendet.

- **Benachrichtigungsgruppe** – Die Nachricht wird an alle Benutzer in der Benutzergruppe gesendet, die dem Bestand zugewiesen ist.
- **Gruppenmanager** – Die Nachricht wird nur an den Benutzer gesendet, der als Gruppenmanager der Benutzergruppe ausgewiesen ist, welche dem Bestand zugewiesen ist. Wenn eine Benutzergruppe keinen ausgewiesenen Gruppenmanager hat, wird keine Nachricht gesendet.
- **Bestimmte Benutzergruppe** – Die Nachricht wird an die ausgewählte Benutzergruppe gesendet. Mit dieser Option können Sie den Alarm steigern, sodass er mehr Benutzer als nur die in der Benutzergruppe, die dem Bestand zugewiesen ist, umfasst.
- **Bestimmter Empfänger** – Die Nachricht wird an eine bzw. mehrere durch Semikolon getrennte E-Mail-Adressen gesendet.
- **Kurznachricht** – Bei Markierung wird eine komprimierte Nachricht gesendet. Zum Beispiel, wenn die Nachricht über ein SMS-Gateway gesendet wird. Bei dieser Option werden die folgenden Informationen entfernt, um die Nachrichtengröße zu erhalten:
  - `%[asset.description]` – Bestandsbeschreibung
  - `%[user.distribution_list]` – Verteilungsliste
  - `%[system.charts]` – Echtzeitdiagramme
  - `%[monitor.dependency_status]` – Abhängigkeitsstrukturstatus
  - `%[monitor.error]` – Monitorfehlermeldung
  - `%[network.contact]` – Netzwerkkontakt

Aktion "Wake-On-LAN-Paket senden"

Die Aktion **Wake-On-LAN-Paket senden** (WOL) kann mit einem Host starten, der den WOL-Standard erfüllt. Informationen dazu, ob die Aktion genutzt werden kann, finden Sie in der Dokumentation des Host.

> **Hinweis:** Diese Aktion ist auf das Aufwecken von Hosts beschränkt, die sich auf derselben *Broadcastdomäne* wie der Host befinden, der zum Senden des WOL-Pakets verwendet wird. Bestände können üblicherweise eine Meldung an alle Bestände übertragen, die denselben Router haben. Router agieren als Grenzen zwischen den Broadcastdomänen. Ein LAN kann mehrere Router beinhalten, wobei jeder Router eine andere Broadcastdomäne darstellt.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Verbinden mit** – `Monitor host` oder `Specific host`. Geben Sie bei einem bestimmten Host die **Mac-Adresse** ein.
- **MAC-Adresse** – Die MAC-Adresse der Schnittstelle, an die das WOL-Paket gesendet werden soll. Das Format der MAC-Adresse ist `AA-BB-CC-DD-EE-FF`. Füllen Sie das Feld nicht aus, wenn Sie die MAC-Adresse des Bestands verwenden möchten.
- **Intervall** – Die Wartezeit in Sekunden zwischen den einzelnen gesendeten Paketen. Wenn die Paketanzahl auf 5 eingestellt ist und das Intervall auf 5, werden in 25 Sekunden 5 Pakete gesendet.
- **Paketanzahl** – Die Anzahl der Paketsendungen. Stellen Sie diesen Wert auf höher als `1` ein, um sicherzugehen, dass der Host das Paket erhält.

Aktion "SNMP-Set"

Die Aktion **SNMP-Set** kann verwendet werden, um die Werte von Bestandsbezeichnern (OIDs) in einem

Remote-SNMP-Agent zu ändern.

Hinweis: Der Communityname (SNMP-Version) und Port, der von **Network Monitor** verwendet wird, um eine Verbindung mit einem SNMP-Bestand zu erstellen, wird in der Registerkarte **Authentifizierung** *(siehe 40)* eines Bestandsknotens festgelegt. Der Bestandsknoten kann diese Einstellung von einem übergeordneten Knoten erben. Siehe **Installationscheckliste** *(siehe 4)*

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Verbinden mit** – `Monitor host` oder `Specific host`. Füllen Sie **Hostname** aus, wenn es einen bestimmten Host gibt.
- **Hostname** – Der Hostname oder die IP-Nummer. Füllen Sie das Feld nicht aus, wenn Sie die Adresse des Bestands verwenden möchten.
- **OID** – Geben Sie die relevante OID ein.
  - Sie können sowohl einen benannte OID als auch eine OID im Zahlenformat angeben. Wenn Sie eine benannte OID angeben, versucht **Network Monitor** automatisch, die OID im Zahlenformat aufzulösen, wenn das Feld den Fokus verliert. **Network Monitor**verwendet für den Versuch, das Zahlenformat der OID zu finden, die aktuell kompilierten MIBs.
  - Die Schaltfläche **[...]** neben dem Feld "OID" zeigt einen MIB-Browser-Dialog an, der zur Auswahl von Bestandsbezeichnern aus dem Remote-SNMP-Agent verwendet werden kann.
  - Wenn der MIB-Browser eine OID-Nummer mit `@string` anzeigt, heißt das, dass Sie diesen String als Teil der OID verwenden können. Zum Beispiel kann die OID `.1.3.6.1.2.1.2.2.1.16@Intel(R) PRO/1000 MT Network Connection` in das OID-Feld eingegeben werden, statt die Indexnummer der Netzwerkverbindung anzugeben.
- **Wert** – Einzustellender Wert.
- **Syntaxtyp** – Werttyp. Der Wert kann eine Ganzzahl oder ein String sein.
- **Anmeldedaten** – `Monitor credentials` oder `Stored credentials`.
- **Anmeldedaten erben** – Wenn gespeicherte Anmeldedaten ausgewählt wurden, wird die Option **Anmeldedaten erben** angezeigt. Bei Markierung werden Anmeldedaten des Bestands vererbt. Geben Sie vorgangsspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diese Aktion verwendet werden.

Ticket-Aktion

Die Aktion **Ticket** erstellt ein Ticket, wenn es durch eine Alarmzählung bei einem Bestand, der von **Network Monitor** überwacht wird, ausgelöst wird. Standardmäßig wird die Aktion **Ticket** von allen Beständen aus dem `KNM`-Gruppenknoten vererbt. Die Alarmzählung ist auf 1 eingestellt.

Hinweis: Ein Ticket wird entweder im Modul **Ticketing** oder in **Service Desk** erstellt, abhängig davon, ob **Service Desk** innerhalb von VSA **aktiviert** *(http://help.kaseya.com/webhelp/DE/KSD/R8/index.asp#5478.htm)* wurde.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Benutzer** – Wählen Sie einen standardmäßigen VSA-Benutzer für die Aktion **Ticket** aus. Es handelt sich um den VSA-Benutzer, der dem erstellten Ticket zugewiesen wurde, wenn kein anderer VSA-Benutzer zugewiesen wurde.

Aktion "Windows-Dienststeuerung"

Die Aktion **Windows-Dienststeuerung** kann Windows-Dienste starten, stoppen, anhalten, fortführen und neu starten. Alle Dienstaktionen verwenden das gleiche Parameter-Set.

Parameter

- **Alarmanzahl** – Die **Anzahl der Alarme** *(siehe 56)*, durch die diese Aktion ausgelöst wird.
- **Verbinden mit** – `Monitor host` oder `Specific host`. Füllen Sie **Hostname** aus, wenn es einen bestimmten Host gibt.
- **Hostname** – Der Hostname oder die IP-Nummer. Füllen Sie das Feld nicht aus, wenn Sie die Adresse des Bestands verwenden möchten.
- **Dienstname** – Der Name des Dienstes. Lassen Sie diese Option leer, um den Dienstnamen vom Monitor abzurufen. Dazu ist es notwendig, dass der Monitor, der diese Aktion ausführt, ein **Windows-Dienststatusmonitor** *(siehe 152)* ist, bei dem nur ein Dienst zur Prüfung konfiguriert ist.
- **Typ** – Wählt den Typ des auszuführenden Vorgangs aus.
  ```
  Continue service
  Pause service
  Start service
  Stop service
  Restart service
  ```
- **Anmeldedaten** – `Monitor credentials` oder `Stored credentials`.
- **Anmeldedaten erben** – Wenn gespeicherte Anmeldedaten ausgewählt wurden, wird die Option **Anmeldedaten erben** angezeigt. Bei Markierung werden Anmeldedaten des Bestands vererbt. Geben Sie vorgangsspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für diese Aktion verwendet werden.

Weitere Informationen siehe auch:

- **Windows-Dienststeuerung** *(siehe 172)* (geplantes Ereignis)
- **Liste der Windows-Dienste** *(siehe 96)* (direkte Steuerung)
- **Windows-Dienststatus** *(siehe 152)* (Monitor)

Informationen zum geplanten Ereignis

Dieses Kapitel enthält Informationen zu allen verfügbaren **geplanten Ereignissen** *(siehe 35)* und deren zugehörigen Einstellungen.

Ereignis "Ereignisprotokoll" löschen

Das Ereignis **Ereignisprotokoll löschen** löscht das Ereignisprotokoll auf einem Remote-Windows-Host.

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Hostname** – Der Hostname des Remotehosts. Dies kann sowohl ein DNS-Name als auch eine IP-Adresse sein.
- **Protokollname** – Geben Sie den Namen des zu löschenden Ereignisprotokolls an.
- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des aktuell markierten Untergruppen- oder Gatewayknotens vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für dieses Ereignis verwendet werden.

Ereignis "Befehl über SSH2/Telnet ausführen"

Das Ereignis **Befehl über SSH2/Telnet ausführen** verbindet sich mit einem Remoteserver über SSH2 oder Telnet und führt einen Befehl aus.

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Hostname** – Der Hostname des Remotehosts. Dies kann sowohl ein DNS-Name als auch eine IP-Adresse sein.
- **Befehl** – Geben Sie den Befehl an, der am Remotehost ausgeführt wird.
- **Port** – Geben Sie die Portnummer für die Verbindung ein. Für SSH2 ist der Standardport 22 und für Telnet 23.
- **Telnet verwenden** – Bei Markierung verbindet sich **Network Monitor** unter Verwendung des Telnetprotokolls mit dem Remotehost. Wenn diese Option aktiviert wird, wird der Port automatisch auf 23 geändert.
- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des aktuell markierten Gruppen- oder Gatewayknotens vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für dieses Ereignis verwendet werden.

Ereignis "Windows-Befehl ausführen"

Das Ereignis **Windows-Befehl ausführen** führt einen bestimmten Befehl **auf dem Network Monitor-Hostrechner aus.** Dies kann verwendet werden, um Skripte oder Batchdateien, die sich auf dem **Network Monitor**-Host befinden, auszulösen. Der Befehl wird als Systembenutzerprozess ausgeführt und kann keine Interaktion mit dem Benutzer anfordern.

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Befehl** – Geben Sie den auszuführenden Befehl ein.

- **Parameter** – Fügen Sie Parameter hinzu, die mit dem Befehl gesendet werden. Verwenden Sie Anführungszeichen, um einen Parameter, der Leerzeichen enthält, als einen Parameter festzulegen.
- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des aktuell markierten Untergruppen- oder Gatewayknotens vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für dieses Ereignis verwendet werden.

Ereignis "Statistiken exportieren"

Das Ereignis **Statistiken exportieren** exportiert gesammelte statistische Daten für eine bestimmte Dauer. Die Daten können für den Import in Tabellenkalkulationsanwendungen in CSV-Dateien (mit Komma getrennte Textdateien) exportiert werden, oder direkt mittels ODBC in eine andere Datenbank. Für den Export in eine andere Datenbank muss ein DSN ODBC-Treiber mit 32 Bit auf dem Rechner der Zieldatenbank konfiguriert werden.

Hinweis: Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereignis "Statistiken"

Die Einstellungen für dieses Ereignis sind in zwei Abschnitte unterteilt. Im ersten Abschnitt werden der Typ und die Quelle der exportierten Daten definiert.

- **Datentyp/Ausgewählte Datentypen** – Wählen Sie den zu exportierenden Datentyp aus. Die Datentypen sind in Kategorien geordnet. Um einen Datentyp zur Exportliste hinzuzufügen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Markieren**. Die ausgewählten Datentypen werden der ausgewählten Liste hinzugefügt. Um einen Datentyp zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Dauer** – Geben Sie den Zeitraum für den Datenexport an.
- **Bestand/Ausgewählte Bestände** – Um Bestände für den Datenexport auszuwählen, wählen Sie zuerst das relevante Netzwerk aus, in dem sich der Bestand befindet. Wählen Sie anschließend einen Bestand oder mehrere Bestände aus der Liste aus und klicken Sie auf die Schaltfläche **Markieren**. Die ausgewählten Bestände werden der ausgewählten Bestandsliste hinzugefügt. Um einen Bestand aus dem Datenexport zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.

Exportoptionen

In diesem Abschnitt werden die Details für die CSV-Datei oder für den Datenbankexport bestimmt.

- **In Datei exportieren** – Wählen Sie diese Option aus, um statistische Daten in eine CSV-Datei zu exportieren.
  - **Dateiname** – Dies ist der Dateiname der exportierten Datei. Dateien werden in das Verzeichnis `KNM\reports\export` exportiert. Fügen Sie optional die folgenden Variablen für die Formatierung ein, wenn Sie den Dateinamen angeben.
    - ✓ `%[system.date]` – das aktuelle Datum
    - ✓ `%[system.time]` – die aktuelle Zeit
- **In Datenbank exportieren** – Wählen Sie diese Option aus, um statistische Daten über ODBC in eine Datenbank zu exportieren.
  - **Datenquellenname** – Der Name einer zuvor festgelegten ODBC-Datenquelle.
  - **Datenbankname** – Der Name der Datenbank, in der die statistischen Informationen gespeichert werden.
- **Tabellen vor dem Export löschen** – Löscht die Datenbanktabellen, bevor die Daten exportiert werden.

- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des aktuell markierten Gruppen- oder Gatewayknotens vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für dieses Ereignis verwendet werden.
- **Markierungsdaten einfügen** – Wenn dies aktiviert ist und es problematisch ist, echte Daten zu liefern, wird stattdessen ein Platzhalterwert von -10.000 eingefügt. Wenn dies deaktiviert ist, ist kein Platzhalterwert eingegeben.

Exportieren von Statistiken in eine CSV-Datei

Wenn statistische Daten in eine Datei exportiert werden, erzeugt **Network Monitor** beim Ausführen des Ereignisses immer zwei Dateien. Die Dateien werden im Ordner `KNM\reports\export` des KNM-Hostrechners gespeichert.

Der Name einer Datei ist im Feld **Dateiname** in den Ereigniseigenschaften festgelegt. Diese Datei enthält die exportierten Rohdaten. Die zweite Datei hat denselben Namen, allerdings mit dem Präfix `info_`. Diese Datei enthält eine Beschreibung der Art der Daten, die exportiert wurden.

Struktur der Informationsdatei:

```
Network name;asset name;monitor
name;monitor-id;monitor-subid;datatype-id;unit;datatype description
```

Beispiel

```
Default network;Backup;Disk utilization (C:);84;0;3;%;Disk utilization
```

Struktur der Datendatei:

```
monitor-id;datatype-id;monitor-subid;timestamp;raw data;comment
```

Beispiel

```
84;3;0;2009/08/05 09:42:57;13.669434;
```

Wenn der Datensatz von **Network Monitor** als ungültig befunden wird, wird der feste Wert -10000.0 exportiert.

Exportieren in eine Datenbank

Wenn statistische Daten in eine Datenbank exportiert werden, erzeugt **Network Monitor** zwei Tabellen in der Datenbank. Die erste Tabelle wird `inmDataExportInformation` genannt. Sie hat die folgende Struktur:

```
CREATE TABLE inmDataExportInformation (networkName char(128), assetName
char(128),monitorName char(128), monitorID integer, atomID integer, dataType
integer, unitNamechar(32), exportedDataType char(128));
```

Diese Tabelle enthält Informationen zu den exportierten Daten, vergleichbar mit dem Export der Daten in eine Datei.

Die zweite Tabelle wird `inmDataExport` genannt. Sie hat die folgende Struktur:

```
CREATE TABLE inmDataExport (monitorID integer, atomID integer, dataType integer,
dataTime DATETIME, dataRaw float);
```

Diese Tabelle enthält alle exportierten statistischen Daten.

Warnung: **Network Monitor** beginnt den Datenexport, indem Tabellen mit diesen beiden Namen abgelegt werden. Der Datenbankbenutzer, der für **Network Monitor** konfiguriert wurde, erfordert angemessenen Zugriff zum ABLEGEN, ERSTELLEN und EINFÜGEN von Vorgängen in der besagten Datenbank. Siehe Datenbankhandbuch, um Informationen zur Konfiguration von Datenbankbenutzern zu erhalten.

Ereignis "Bericht generieren"

Das Ereignis **Bericht generieren** wird verwendet, um die Generierung eines Berichts zu planen sowie um den Bericht an bestimmte Empfänger zu senden oder diesen zu veröffentlichen.

Hinweis: Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Registerkarte "Ereigniskonfiguration"

Bericht generieren

Wählen Sie den zu generierenden Berichtstyp aus.

- **Benutzerdefinierten Bericht generieren** – Wenn diese aktiviert ist, wurden bereits alle Konfigurationseinstellungen sowie alle Bestands- und Monitorauswahlen unter Verwendung von Network Monitor-Berichten > **Berichte anpassen** *(siehe 79)* ausgeführt. Sie müssen nur den Namen des benutzerdefinierten Berichts in der Dropdownliste **Benutzerdefinierter Bericht** auswählen.
- **Berichtsvorlage generieren** – Wenn dies aktiviert ist, müssen Sie die zu verwendende Berichtsvorlage, die Zeitperiode und die Bestände und Monitore auswählen, die in den Bericht eingefügt werden.
  - **Berichtsvorlage** – Wählen Sie eine Berichtsvorlage zum Planen aus. Siehe Abschnitt unten zur Auswahl von Beständen für eine Berichtsvorlage.
  - **Dauer** – Wählen Sie die Berichtsperiode für die Berichtsvorlage aus.
  - **Ausführen als** – Wählen Sie den Benutzer aus, der den Bericht ausführt.
  - **Berichte trennen** – Wählen Sie diese Option aus, um Berichte für jeden Bestand getrennt zu versenden.

Auswahl

Dieser Abschnitt erscheint nur, wenn **Berichtsvorlage generieren** ausgewählt wurde. Legen Sie fest, welche Bestände im Bericht eingefügt werden.

- **Bestand auswählen/Ausgewählte Bestände** – Geben Sie Text ein, um die Namen der Bestände in der Liste **Bestand auswählen** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie einen Bestand oder mehrere Bestände in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um den Bestand der Liste **Ausgewählte Bestände** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielbeständen zu suchen. Um einen Bestand zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Monitor auswählen/Ausgewählte Monitore** – Geben Sie Text ein um die Namen der Monitore in der Liste **Monitor auswählen** anzuzeigen, die dem eingegebenen Text entsprechen. Wählen Sie ein oder mehrere Monitore in der Liste aus. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**, um die Monitore der Liste **Ausgewählte Gruppen** hinzuzufügen. Sie können auch auf die Schaltfläche **Markieren** klicken, um nach den Zielmonitoren zu suchen. Um einen Monitor zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.

Registerkarte "Berichtsempfänger"

Verwenden Sie diesen Abschnitt, um die Empfänger für den generierten Bericht auszuwählen.

- **Benutzergruppe** – Wählen Sie eine Benutzergruppe aus der Liste aus und klicken Sie auf die Schaltfläche **Markieren**. Sie können mehrere Gruppen einfügen. Die ausgewählten Benutzergruppen werden der ausgewählten Gruppenliste hinzugefügt. Um eine Benutzergruppe zu entfernen, wählen Sie diese aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Benutzer** – Wählen Sie den Benutzer aus der Liste aus und klicken Sie auf die Schaltfläche **Markieren**. Sie können mehrere Benutzer einfügen. Der ausgewählte Benutzer wird der ausgewählten Benutzerliste hinzugefügt. Um einen Benutzer zu entfernen, wählen Sie diesen aus und klicken Sie auf die Schaltfläche **Entfernen**.

- **E-Mail** – Geben Sie einzelne E-Mail-Adressen als Empfänger an. Trennen Sie mehrere Einträge mit einem Komma voneinander.
- **Betreff** – Legen Sie eine Betreffzeile für den per E-Mail versendeten Bericht fest. Wenn dies nicht ausgefüllt wird, wird ein standardmäßiges Format für die Betreffzeile verwendet, das in der Registerkarte Network Monitor-Einstellungen > SMS > **Standardnachrichten** *(siehe 113)* festgelegt ist.
- **Verzeichnis** – Der generierte Bericht kann in einem Netzwerkordner als HTML-Dokument veröffentlicht werden. Geben Sie den Pfad zu diesem Ordner an. Fügen Sie optional die folgenden Variablen für die Formatierung ein, wenn Sie den Pfad angeben.
  - `%[system.date]` – aktuelles vollständiges Datum
  - `%[system.date_year]` – aktuelles Jahr
  - `%[system.date_month]` – aktueller Monat
  - `%[system.date_day_of_month]` – aktueller Monatstag
  - `%[system.time]` – aktuelle vollständige Zeit
  - `%[system.time_hour]` – aktuelle Stunde
  - `%[system.time_minute]` – aktuelle Minute
  - `%[system.time_second]` – aktuelle Sekunde

Optionen zum Hochladen auf FTP

Der generierte Bericht kann auf einem FTP-Server als HTML-Dokument veröffentlicht werden.

- **FTP-Host & Port** – Legen Sie den Hostnamen und die Portnummer fest. Standardeinstellungen `21`.
- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des aktuell markierten Gruppen- oder Gatewayknotens vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für dieses Ereignis verwendet werden.

Ereignis "HTTP GET/POST-Anfrage"

Das Ereignis **HTTP GET/POST-Anfrage** führt eine HTTP-Anfrage an einen Remotehost aus. Die beiden Anfragemethoden GET und POST werden unterstützt.

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **URL** – Geben Sie die Ziel-URL für die Anfrage an.
- **SSL** – Bei Markierung verwendet die Anfrage Secure Socket Layer (SSL). Wenn diese Option aktiviert wird, wird die Portnummer automatisch aktualisiert.
- **Port** – Geben Sie die zu verwendende Portnummer an. Der Standardport für HTTP ist 80.
- **Parameter** – *Nur bei POST-Anfragen.* Geben Sie Parameter im Format `name=value` ein, ein Parameter pro Zeile. Die folgenden **Formatierungsvariablen** *(siehe 66)* können Teil eines Parameters sein.
  - `%[system.time]` – aktuelle Zeit
  - `%[asset.name]` – Bestandsname
  - `%[asset.address]` – Bestandsadresse
  - `%[monitor.name]` – Monitorname
  - `%[monitor.error]` – Monitorfehlermeldung
  - `%[monitor.error2]` – Monitorfehlermeldung, kein Zeitstempel

  - `%[asset.description]` – Bestandsbeschreibung
  - `%[group.name]` – Gruppenname
  - `%[group.contact]` – Gruppenkontakt
- **Zeichencodierung** – `ISO-8859-1` oder `UTF-8`. Die von der Anfrage verwendete Codierung.
- **HTTP-Authentifizierung** – Geben Sie, wenn dies markiert ist, Anmeldedaten ein, um die Anfrage zu authentifizieren.
- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des aktuell markierten Gruppen- oder Gatewayknotens vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für dieses Ereignis verwendet werden.
- **Proxy-Einstellungen**
  - **Proxy-Server** – Adresse des Proxy-Servers.
  - **Proxy-Port** – Portnummer des Proxy-Servers.

Ereignis "Lua-Skripte"

Das Ereignis **Lua-Skripte** führt ein Lua-Skript aus. Lua ist die Skriptsprache, die ursprünglich von **Network Monitor** unterstützt wird. Weitere Informationen finden Sie unter **Lua** *(siehe 205)*.

Hinweis: Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Skript** – Wählen Sie das auszuführende Skript aus. Lua-Skripte, die mit **Network Monitor** verwendet werden, müssen im Ordner `KNM\scripts` des KNM-Hostrechners gespeichert werden. Sobald ein Skript ausgewählt wurde, erscheinen für die Skriptparameter verschiedene Felder.
- **Anmeldedaten**
  - `No authentication` – Keine Anmeldedaten erforderlich.
  - `Use specific credentials in API` – Legt einen **Kontotyp** für `Windows domain account`, `SSH/Telnet account` oder `VMware account` fest. Wenn diese Option ausgewählt wird, führt **Network Monitor** keine Windows-Authentifizierung durch, bevor das Skript ausgeführt wird. Stattdessen werden die angegebenen Kontoanmeldeinformationen als Parameter an das Skript weitergegeben. Dies ist sinnvoll bei Skripten, die benutzerdefinierte Anmeldungen durchführen wollen, z. B. mit SSH2.
  - `Perform Windows impersonation` – Eine Windows-Authentifizierung wird mit dem angegebenen Host durchgeführt, bevor das Skript ausgeführt wird. Dies ist sinnvoll bei Skripten, für die eine Authentifizierung vor der Ausführung erforderlich ist.
- **Anmeldedaten erben** – Wenn `Use specific credential in API` oder `Perform Windows impersonation` aktiviert sind, wird die Option **Anmeldedaten erben** angezeigt. Bei Markierung werden Anmeldedaten des Gruppen- oder Gatewayknotens vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für dieses Ereignis verwendet werden.

Ereignis "E-Mail senden"

Das Ereignis **E-Mail senden** sendet eine E-Mail mit festgelegtem Inhalt an einen bzw. mehrere Benutzer

oder an Benutzergruppen. Weitere Informationen zum Konfigurieren von E-Mail-Einstellungen siehe Abschnitt E-Mail- und SMS-Einstellungen.

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Benutzergruppe** – Wählen Sie eine Benutzergruppe aus, die die Nachricht empfangen wird.
- **Benutzer/Ausgewählte Benutzer** – Fügen Sie bestimmte Benutzer als Empfänger der Nachricht hinzu, indem Sie diese in der Liste auswählen und auf die Schaltfläche **Markieren** klicken. Um einen Benutzer zu entfernen, wählen Sie diesen aus der Liste aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Bestimmter Empfänger** – Geben Sie bestimmte E-Mail-Adressen ein. Trennen Sie mehrere Einträge mit einem Komma voneinander.
- **Betreff** – Legen Sie die Betreffzeile der Nachricht fest.
- **Meldung** – Legen Sie den Text der Mitteilung fest.

Ereignis "Nachricht über PageGate senden"

Das Ereignis **Nachricht über PageGate senden** sendet eine Paging-Nachricht an einen bzw. mehrere Benutzer oder an Benutzergruppen über einen PageGate-Paging-Server. Weitere Informationen zum Konfigurieren von PageGate siehe Abschnitt **Verschiedene Einstellungen** *(siehe 109)*.

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Benutzergruppe** – Wählen Sie eine Benutzergruppe aus, die die Nachricht empfangen wird.
- **Benutzer/Ausgewählte Benutzer** – Fügen Sie bestimmte Benutzer als Empfänger der Nachricht hinzu, indem Sie diese in der Liste auswählen und auf die Schaltfläche **Markieren** klicken. Um einen Benutzer zu entfernen, wählen Sie diesen aus der Liste aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Bestimmter Empfänger** – Geben Sie einen bestimmten PageGate-Benutzer ein. Trennen Sie mehrere Einträge mit einem Komma voneinander.
- **Betreff** – Legen Sie die Betreffzeile der Nachricht fest.
- **Meldung** – Legen Sie den Text der Mitteilung fest.

Ereignis "SMS senden"

Das Ereignis **SMS senden** sendet eine SMS-Nachricht mit festgelegtem Inhalt an einen bzw. mehrere Benutzer oder an Benutzergruppen. Weitere Informationen zum Konfigurieren eines SMS-fähigen Bestands siehe Abschnitt E-Mail- und SMS-Einstellungen.

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Benutzergruppe** – Wählen Sie eine Benutzergruppe aus, die die Nachricht empfangen wird.
- **Benutzer/Ausgewählte Benutzer** – Fügen Sie bestimmte Benutzer als Empfänger der Nachricht hinzu, indem Sie diese in der Liste auswählen und auf die Schaltfläche **Markieren** klicken. Um einen Benutzer zu entfernen, wählen Sie diesen aus der Liste aus und klicken Sie auf die Schaltfläche **Entfernen**.

- **Bestimmter Empfänger** – Geben Sie bestimmte Telefonnummern ein. Trennen Sie mehrere Einträge mit einem Komma voneinander.
- **Betreff** – Legen Sie die Betreffzeile der Nachricht fest.
- **Meldung** – Legen Sie den Text der Mitteilung fest.

Ereignis "Wake-On-LAN-Paket senden"

Das Ereignis **Wake-On-LAN-Paket senden** kann einen Remotehost unter Verwendung des Wake-On-LAN-Pakets hochfahren. Um dieses Ereignis zu verwenden, muss der Remotehost die Wake-On-LAN-Funktion unterstützen.

Hinweis: Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **MAC-Adresse** – Legen Sie die MAC-Adresse der Netzwerkkarte auf dem Remotehost fest, die die Wake-On-LAN-Anfrage erhält. Das Format der MAC-Adresse ist `AA-BB-CC-DD-EE-FF`.
- **Intervall** – Die Wartezeit in Sekunden, zwischen den einzeln gesendeten Paketen. Wenn die Paketanzahl auf 5 eingestellt ist und das Intervall auf 5, werden in 25 Sekunden 5 Pakete gesendet.
- **Paketanzahl** – Die Anzahl der Paketsendungen. Stellen Sie diesen Wert auf höher als `1` ein, um sicherzugehen, dass der Host das Paket erhält.

Ereignis "SNMP-Set"

Das Ereignis **SNMP-Set** sendet eine SNMP-Set-Anfrage an einen Remote-SNMP-Agent.

Hinweis: Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Hinweis: Der Communityname (SNMP-Version) und Port, der von **Network Monitor** verwendet wird, um eine Verbindung mit einem SNMP-Bestand zu erstellen, wird in der Registerkarte **Authentifizierung** *(siehe 40)* eines Bestandsknotens festgelegt. Der Bestandsknoten kann diese Einstellung von einem übergeordneten Knoten erben. Siehe **Installationscheckliste** *(siehe 4)*

Ereigniseinstellungen

- **Hostname** – Der Hostname des Remote-SNMP-Agent. Dies kann sowohl ein DNS-Name als auch eine IP-Adresse sein.
- **OID** – Geben Sie den relevanten OID ein.
  - Sie können sowohl einen benannte OID als auch eine OID im Zahlenformat angeben. Wenn Sie einen benannten OID angeben, versucht **Network Monitor** automatisch, die OID im Zahlenformat aufzulösen, wenn das Feld den Fokus verliert. **Network Monitor**verwendet für den Versuch, das Zahlenformat der OID zu finden, die aktuell kompilierten MIBs.
  - Die Schaltfläche **[...]** neben dem OID-Feld zeigt einen MIB-Browserdialog an, der verwendet werden kann, um Bestandsbezeichner vom Remote-SNMP-Agent auszuwählen.
  - Wenn der MIB-Browser eine OID-Nummer mit `@string` anzeigt, heißt das, dass Sie diesen String als Teil des OID verwenden können. Zum Beispiel kann der OID `.1.3.6.1.2.1.2.2.1.16@Intel(R) PRO/1000 MT Network Connection` in das OID-Feld eingegeben werden, anstatt die Indexnummer der Netzwerkverbindung anzugeben.
- **Wert** – Einzustellender Wert.
- **Syntax** – Werttyp. Der Wert kann eine Ganzzahl oder ein String sein.

- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten der Gruppe vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **SNMP-Version/Community lesen/Community schreiben** – Anmeldedaten, die zur Zugriffsauthentifizierung und zur Ausführung des Ereignisses **SNMP-Set** verwendet werden.

Ereignis "Monitor auslösen"

Das Ereignis **Monitor auslösen** kann verwendet werden, um zu einem bestimmten Zeitpunkt einen Monitortest auszuführen. Dies kann für Monitore hilfreich sein, die nur zu bestimmten Zeitpunkten getestet werden dürfen. *Sobald ein Test für einen Monitor geplant ist, wird der Monitor nicht mehr wie sonst regelmäßig getestet.*

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Monitor** – Wählen Sie den auszulösenden Monitor aus.

Ereignis "Windows-Dienststeuerung"

Das Ereignis **Windows-Dienststeuerung** kann den Status des Windows-Dienstes auf einem Remotehost ändern.

> **Hinweis:** Eine Einführung zum Planen von Ereignissen finden Sie unter **Registerkarte "Zeitpläne"** *(siehe 35)*.

Ereigniseinstellungen

- **Hostname** – Der Hostname des Remotehosts. Dies kann sowohl ein DNS-Name als auch eine IP-Adresse sein.
- **Dienstname** – Geben Sie den Namen des Dienstes an. Es muss sich um den Dienstnamen und nicht um den Anzeigenamen handeln.
- **Typ** – Wählt den Typ des auszuführenden Vorgangs aus.
  ```
  Continue service
  Pause service
  Start service
  Stop service
  Restart service
  ```
- **Anmeldedaten erben** – Bei Markierung werden Anmeldedaten des aktuell markierten Untergruppen- oder Gatewayknotens vererbt. Geben Sie ereignisspezifische Anmeldedaten ein, wenn dies deaktiviert ist.
- **Domäne oder Computer/Benutzername/Passwort** – Anmeldedaten, die zur Zugriffsauthentifizierung für dieses Ereignis verwendet werden.

Weitere Informationen siehe auch:

- **Windows-Dienststeuerung** *(siehe 163)* (Aktion)
- **Liste der Windows-Dienste** *(siehe 96)* (direkte Steuerung)
- **Windows-Dienststatus** *(siehe 152)* (Monitor)

Kapitel 5

Weiterführende Informationen

In diesem Kapitel

Init.cfg-Parameter 174
Backup und Wiederherstellung 175
Datenextrahierungsreferenz 176
UNIX-Systemunterstützungsdateien 183
Aktivierung des ODBC-Treibers 185

Init.cfg-Parameter

Die Datei `Init.cfg` wird von **Network Monitor** für Einstellungen verwendet, die erforderlich sind, bevor die Datenbank mit der Konfiguration geladen wird. Sie steuert, auf welchem Port **Network Monitor** den Webserver startet und in welchem Modus (Standard, Verteilter Server oder Verteiltes Gateway) **Network Monitor** startet. Die Datei `Init.cfg` befindet sich im KNM-Stammverzeichnis.

Protokoll

- `PROTOKOLLIERUNGSSTUFE = 0` – Protokollierungsstufe; wird diese auf einen anderen Wert als Null eingestellt, schreibt **Network Monitor** Debuginformationen in das Textprotokoll. Gültige Protokollierungsstufen sind 0, 1 und 2. Wird die Protokollierungsstufe auf 2 eingestellt (Standardeinstellung ist 1), beginnt **Network Monitor**, detaillierte Informationen in einer `<Kaseya_Installation_Directory>\Logs\Services\KaseyaNetworkMonitor.log`-Datei zu protokollieren. Dies kann beispielsweise beim Debuggen des Mail- und SMS-Sendeverhaltens nützlich sein. Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.

SSH2

- `SSH2_ZEITLIMIT=25000` - SSH2-Client-Zeitlimit in Millisekunden. Standardeinstellung `25000` (25 Sekunden). Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.
- `SSH2_ABLAUFVERFOLGUNGSEBENE=0` - Die Ablaufverfolgungsebene kann zum Debuggen der SSH2-Verbindung verwendet werden. Die Standardeinstellung ist `0`. Gültiger Bereich: 0 bis 4 (max. Ausgabe). Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.

Testen der Threadpoolkonfiguration

- `TP_INIT_GRÖSSE` – Die ursprüngliche Größe des Threads. Die Standardeinstellung ist `20`.
- `TP_MAX_AGE` – Das maximale Alter in Sekunden, bis zu dem ein Thread ungenutzt bleiben kann, ohne aus dem Pool gelöscht zu werden. Die Standardeinstellung ist `3600` (eine Stunde). Der Zweck dieses Parameters besteht darin, die Größe des Threadpools so auszubalancieren, dass diese optimal für Ihre Konfiguration ist.
- `TP_MAX_GRÖSSE` – Die maximale Größe, auf die der Threadpool anwachsen kann. Die Standardeinstellung ist `125`.

Andere

- `OBJEKT_IP_CACHE=1` - **Network Monitor** löst alle Hostnamen von Beständen in IP-Adressen auf. Diese Funktion kann deaktiviert werden, falls es Probleme mit dem lokalen DNS gibt. Die Standardeinstellung ist `1` (aktiviert). Optional `0` (deaktiviert). Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.
- `DELAY_TEST_START=0` – Dieser Parameter kann verwendet werden, um beim Start von **Network Monitor** den Start von Monitortests zu verzögern. Die Standardeinstellung ist `0` Sekunden. Indem mithilfe dieses Parameters der Start von **Network Monitor**-Monitortests verzögert wird, lässt sich die Bootzeit von Rechnern reduzieren. Es können keine Änderungen vorgenommen werden, solange **Network Monitor** ausgeführt wird.
- `OPERATOR_SESSION_TIMEOUT=20` – Legt das Zeitlimit für eine Benutzersitzung (in Minuten) fest. Ist kein Zeitlimit erwünscht, setzen Sie den Wert auf -1. Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.
- `SNMP_TIMEOUT=10000` – Legt das Zeitlimit (in Millisekunden) für alle SNMP-Funktionen (Monitore, Aktionen usw.) fest. Standardeinstellung: 10 Sekunden. Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.

- `ENABLE_CRASHFILE=wahr` – Ist dieser Parameter aktiviert und befindet sich **Network Monitor** in einer Deadlock-Situation, erzeugt **Network Monitor** im KNM-Stammverzeichnis eine Absturzabbilddatei namens `crash.now`. Diese Datei wird von **Network Monitor**-Entwicklern genutzt, um zu analysieren, warum der Deadlock aufgetreten ist. Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.
- `DISTTEST_UPDATE_INTERVAL=60` – Zeit zwischen Ereignissen, die das Gateway und den Server dazu veranlassen, Informationen auszutauschen. Kann in den `Init.cfg`-Dateien von Gateway und Server auf unterschiedliche Werte festgelegt werden. Als Standardeinstellung werden 60 Sekunden empfohlen.
- `DISABLE_RTS` – Ist diese Variable vorhanden und wird sie in der `Init.cfg`-Datei so festgelegt, dass sie beim Start 1 beträgt, so werden keine Echtzeitstatistiken für Monitore geladen. Dadurch lässt sich das Starten von **Network Monitor** beträchtlich beschleunigen.
- `NO_TESTING` – Ist diese Variable vorhanden und wird sie in der `Init.cfg`-Datei so eingestellt, dass sie beim Start 1 beträgt, so werden so lange keine Tests durchgeführt, bis ein Benutzer die Tests wieder aktiviert.
- `HOSTNAME_OVERRIDE=myhost.domain.local` – Beim Senden von Benachrichtigungen an Benutzer wird eine Verknüpfung zum Monitor/Bestand in die Benachrichtigungs-E-Mail integriert. Die Verknüpfung beginnt mit dem Hostnames des **Network Monitor**-Hostrechners. Dieser Parameter kann dazu verwendet werden, diesen Namen zu überschreiben. Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.
- `DISTTEST_MODE=server` – Dieser Parameter veranlasst **Network Monitor** dazu, das verteilte Subsystem entweder im "Server"-Modus oder im "Gateway"-Modus zu starten. Dieser Parameter ist vom Parameter `DISTTEST_ENABLE` abhängig. Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.
- `DISTTEST_ENABLE=1` – Dieser Parameter veranlasst **Network Monitor** dazu, das verteilte Subsystem zu starten. Dieser Parameter ist vom Parameter `DISTTEST_MODE` abhängig. Dieser Parameter kann entweder auf 1 (aktivieren) oder auf 0 (deaktivieren) gesetzt werden. Änderungen können vorgenommen werden, während **Network Monitor** ausgeführt wird.

Backup und Wiederherstellung

In diesem Abschnitt erfahren Sie, wie Sie ein vollständiges Backup von **Network Monitor** machen und wie Sie die Konfiguration wiederherstellen.

Backup von Network Monitor

Network Monitor erstellt in regelmäßigen Abständen ein Backup der Hauptkonfigurationsdatenbank, `settings.rds` und der zugehörigen Konfigurationsdatei, `server.nxd`. Diese Backups werden im Verzeichnis `KNM\backup` des KNM-Hostrechners gespeichert.

> **Hinweis:** Es liegt in der Verantwortung des Kunden, Backups dieser und anderer Dateien, aus denen die Installation von **Network Monitor** besteht, zu erstellen.

Ein Backup sollte die folgenden Dateien und Verzeichnisse umfassen:

- `\backup`
- `\rmstorage` - Das Verzeichnis `\rmstorage` ist das Standardverzeichnis. Falls Sie den Kaseya Record Manager auf einem anderen Computer installiert haben oder ihn so konfiguriert haben, dass er ein anderes Verzeichnis nutzt, erstellen Sie stattdessen ein Backup dieses Verzeichnisses.
- `\dashboard`
- `\script`
- `\gateways`

- `\system`
- `settings.rds`
- `toplist.rds`
- `server.nxd`
- `init.cfg`

Wiederherstellen der Konfiguration

Network Monitor erstellt in regelmäßigen Abständen automatische Backups der Datenbank. Die Dateien werden zusammen mit einer Kopie der Datei `server.nxd` im Ordner `KNM\backup` des KNM-Hostrechners gespeichert. Das Dienstprogramm zum Wiederherstellen der Befehlszeile ist in der Lage, die aktuelle Konfiguration durch ein Backup zu ersetzen.

> **Warnung:** Durch das Wiederherstellen einer älteren Version Ihrer Konfiguration wird die aktuelle Konfiguration überschrieben.

1. Fahren Sie **Network Monitor** herunter.
2. Erstellen Sie ein Backup der Dateien `settings.rds` und `server.nxd`.
3. Entfernen Sie die Dateien `settings.rds` und `server.nxd` aus dem Verzeichnis `KNM`.
4. Kopieren Sie die Datei `server-YYYY-MM-DD.bak` aus dem Verzeichnis `\backup` und benennen Sie sie in `server.nxd` um.
5. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zu Ihrem `KNM`-Verzeichnis.
6. Geben Sie folgenden Text in die Eingabeaufforderung ein und drücken Sie dann die Taste "Enter".

```
nmservice.exe -restore backup\settings-YYYY-MM-DD.bak
```

Network Monitor stellt die `settings.rds`-Datenbank aus der Datei `settings-YYYY-MM-DD.bak` wieder her.

> **Hinweis:** Es ist sehr wichtig, dass die Dateien `settings-YYYY-MM-DD.bak` und `server-YYYY-MM-DD.bak`, die Sie bei diesem Vorgang verwenden, *dasselbe Datum aufweisen.*

Datenextrahierungsreferenz

Über die Datenextrahierungsoberfläche können Sie mithilfe von "HTTP Get'-Befehlen Daten aus **Network Monitor** extrahieren.

Voraussetzung

Jede an **Network Monitor** gesendete "Get'-Anfrage muss einen Benutzernamen enthalten. Ist der Benutzer auch als Systemadministrator gekennzeichnet, hat er Zugriff auf das gesamte System. Andernfalls hat der Benutzer lediglich Zugriff auf Daten, für die die Benutzergruppen, denen er angehört, Zugriffsrechte haben. Ist der Benutzer nicht berechtigt, auf bestimmte Informationen zuzugreifen, gibt **Network Monitor** den Fehlercode "HTTP 404" aus.

URL-Syntax

Das Format der an **Network Monitor** gesendeten URL muss einige bestimmte Parameter aufweisen.

Beispiel-URL für die Extrahierung einer Grafik aus einem Monitor

```
http://localhost/knm/extract.xsi?cmd=monitor_graph&user=Admin&id=8&param1=2
```

cmd	Auszuführender Befehl
user	**Network Monitor** user username
id	ID des Monitors oder des Benutzers
param1	Benutzerdefinierter Parameter

dir

Verwenden Sie den Befehl `dir`, um eine Liste der verfügbaren Monitore und Benutzer einschließlich Namen und IDs zu erhalten. Dieser Befehl ist besonders nützlich, wenn Sie Extrahierungs-URLs für alle anderen Befehle festlegen.

Syntax

```
http://localhost/knm/extract.xsi?cmd=dir&user=Admin
```

cmd	dir
user	Network Monitor user username

Ausgegebene Daten

Eine Liste der Monitore und Benutzer mit deren IDs.

monitor_graph

Verwenden Sie den Befehl `monitor_graph`, um eine PNG-Bilddatei mit der ausgewählten Echtzeitgrafik zu erhalten. Es handelt sich dabei exakt um diejenige Grafik, die auf der Seite **Monitorinformationen** angezeigt wird. Bevor eine Grafik extrahiert werden kann, muss sie zunächst über die Seite **Monitorinformationen** aktiviert werden.

Syntax

```
http://localhost/knm/extract.xsi?cmd=monitor_graph&user=Admin&id=8&param1=2&deviceid=2
```

cmd	monitor_graph
user	KNM user username
id	ID des Monitors
param1	Nullbasierter Index der abzurufenden Grafik. Der Index basiert auf aktivierten Grafiken.
deviceid	Bestands-ID

Ausgegebene Daten

Eine PNG-Bilddatei mit einer Standardgröße von 747x120 Pixeln und einer Farbtiefe von 3 Byte pro Pixel.

monitor_status_list

Verwenden Sie den Befehl `monitor_status_list`, um eine Monitor-Statuszeichenfolge zu erhalten. Es handelt sich dabei exakt um diejenige Statuszeichenfolge, die auf der Seite **Monitorinformationen** angezeigt wird.

Syntax

```
http://localhost/knm/extract.xsi?cmd=monitor_status_list&user=Admin&deviceid=2
```

cmd	monitor_status_list
user	KNM user username
deviceid	Bestands-ID

Ausgegebene Daten

Eine Zeichenfolge mit dem Namen des Bestands und des Monitors, die Statuszeichenfolge und der Status des Monitors (getrennt durch einen senkrechten Strich: `|`). Die einzelnen Zeilen sind durch Zeilenumbrüche voneinander getrennt.

Beispiel

```
MyAsset | CPU load Monitor | Current CPU usage 11.00 % | OK
MyAsset | Memory size Monitor | Free memory 256 MB | FAILED
```

monitor_statusstring

Verwenden Sie den Befehl `monitor_statusstring`, um eine Monitor-Statuszeichenfolge zu erhalten. Es handelt sich dabei exakt um diejenige Statuszeichenfolge, die auf der Seite **Monitorinformationen** angezeigt wird.

Syntax

```
http://localhost/knm/extract.xsi?cmd=monitor_statusstring&user=Admin&id=8&deviceid=2
```

cmd	monitor_statusstring
user	KNM user username
id	ID des Monitors
deviceid	Bestands-ID

Ausgegebene Daten

Eine Zeichenfolge mit dem Namen des Monitors, die Statuszeichenfolge und der Status des Monitors (getrennt durch einen senkrechten Strich: `|`).

Beispiel

```
CPU load Monitor | Current CPU usage 11.00 % | OK
```

monitor_uptimestring

Verwenden Sie den Befehl `monitor_uptimestring`, um eine Zeichenfolge zu erhalten, die Auskunft über die Monitorbetriebszeit gibt. Die Betriebszeit-Zeichenfolge enthält die Betriebszeit des Monitors in Stunden, Minuten und Sekunden. Befindet sich der Monitor im Alarmstatus, ist der Zeichenfolge ein Sternchen (`*`) vorangestellt, das darauf hinweist, dass die Zeichenfolge die Ausfallzeit des Monitors angibt.

Syntax

```
http://localhost/knm/extract.xsi?cmd=monitor_uptimestring&user=Admin&id=8&deviceid=2
```

cmd	monitor_uptimestring
user	KNM user username

id	ID des Monitors
deviceid	Bestands-ID

Ausgegebene Daten

Eine Zeichenfolge mit dem Namen des Monitors und eine Zeichenfolge mit der Betriebs-/Ausfallzeit (getrennt durch einen senkrechten Strich: `|`).

Beispiel

```
CPU load Monitor | 0h 59m 35s
```

device_xml

Verwenden Sie den Befehl `device_xml`, um ein XML-Dokument mit Informationen zu einem Bestand zu erhalten. Um auf den jeweiligen Bestand zugreifen zu können, muss der Benutzer Mitglied der Benutzergruppe sein, die dem Bestand zugeordnet ist.

Syntax

```
http://localhost/knm/extract.xsi?cmd=device_xml&user=Admin&id=2
```

cmd	device_xml
user	KNM user username
id	ID des Bestands

Ausgegebene Daten

Ein XML-Dokument.

XML-Felder

DEVICE	Stamm der Baumstruktur
NAME	Tatsächlicher Name
DESC	Beschreibung des Bestands
IP_ADDRESS	IP-Adresse oder Hostname des Bestands
MAC_ADDRESS	MAC-Adresse des Bestands (falls vorhanden)
ACTIVE	"YES" (JA), falls der Bestand aktiviert ist; "NO" (NEIN), falls er deaktiviert ist
MAINTENANCE	"Available" (Verfügbar), falls der Benutzer eingeplant und im Dienst ist; "n/a" (Nicht verfügbar), falls der Benutzer nicht eingeplant oder nicht im Dienst ist
MONITOR	Dem Bestand untergeordnet
NAME	Monitorname
TEST_INTERVAL	Intervall zwischen Tests (in Sekunden)
ALARM_DELAY	Intervall zwischen Tests, wenn der Monitor sich im Alarmstatus befindet (in Sekunden)
ALARM_GENERATION	Zahl, die angibt, wie viele aufeinanderfolgende Tests fehlschlagen müssen, damit ein Monitor in den Alarmstatus versetzt wird
LAST_TEST	Zeitpunkt des letzten Tests
LAST_OK_TEST	Zeitpunkt des letzten erfolgreich ausgeführten

	Tests
LAST_FAILED_TEST	Zeitpunkt des letzten fehlgeschlagenen Tests
TEST_DONE	Anzahl der ausgeführten Tests seit dem letzten Neustart
ACTIVE	"YES" (JA), falls der Monitor aktiviert ist; "NO" (NEIN), falls er deaktiviert ist
TYPE	Monitortyp
STATUS	Status des Monitors – kann "OK", "FAILED" (Fehlgeschlagen) oder "ALARM" sein
STATUS_STRING	Die letzte Statuszeichenfolge
UPTIME	Zeit, während der sich der Monitor im Status "OK" oder im Status "ALARM" befand (falls die Zeichenfolge im Alarmstatus mit dem Präfix "*" versehen ist)
INM_ALARM_MESSAGE	Dem MONITOR untergeordnet; zeigt die letzten fünf Statuszeichenfolgen
MESSAGE	Statustext
TIME	Zeitpunkt des Eintrags
STATUS	"OK", "FAILED" (Fehlgeschlagen) oder "ALARM"
INM_GRAPH_LINK	Dem MONITOR untergeordnet; enthält Informationen zu den Echtzeitgrafiken, die auf der Seite "Monitorinformationen" angezeigt werden
LINK	Eine Datenextrahierungsverknüpfung zur Grafik
DESC	Beschreibung der Grafik
UNIT	Einheit der Y-Achse der Grafik
PERIOD	Zeitperiode, die die Grafik umfasst
STATUS_EX	Erweiterter Status für SNMP-, SSH2 Script-, ODBC- und WinPerf-Monitore
STATUS	Status des Monitors – kann "OK", "FAILED" (Fehlgeschlagen) oder "ALARM" sein
UNIT	Benutzerdefinierte Einheit
COMPARE_VALUE	Benutzerdefinierter Wert, mit dem der Wert aus einem Test verglichen wird, um das Testergebnis bewerten zu können
COMPARE_OPERATION	Vorgang, im Rahmen dessen der Wert aus einem Test mit dem benutzerdefinierten Vergleichswert verglichen wird Kann sein: • EQUAL (Gleich) • NOT EQUAL (Nicht gleich) • GREATER (Größer) • LESS (Kleiner) • EQUAL OR GREATER (Größer oder gleich) • EQUAL OR LESS (Kleiner oder gleich)

LAST_VALUE	Letzter Wert, der sich aus einem Test ergeben hat

Beispiel

```
<DEVICE>
   <NAME>DOMAINSERVER</NAME>
   <DESC></DESC>
   <IP_ADDRESS>192.168.1.1</IP_ADDRESS>
   <MAC_ADDRESS>00-00-5A-A8-07-D8</MAC_ADDRESS>
   <ACTIVE>YES</ACTIVE>
   <MAINTENANCE>NO</MAINTENANCE>
   <MONITOR>
           <NAME>Bandwidth test</NAME>
           <TEST_INTERVAL>10</TEST_INTERVAL>
           <ALARM_DELAY>600</ALARM_DELAY>
           <ALARM_GENERATION>5</ALARM_GENERATION>
           <LAST_TEST>2004-06-10 13:38:55</LAST_TEST>
           <LAST_OK_TEST>2004-06-10 13:38:40</LAST_OK_TEST>
           <TEST_DONE>0</TEST_DONE>
           <ACTIVE>NO</ACTIVE>
           <TYPE>Bandwidth test</TYPE>
           <STATUS>OK</STATUS>
           <STATUS_STRING></STATUS_STRING>
           <UPTIME>23t 4m 45s</UPTIME>
   </MONITOR>
</DEVICE>
```

devicelist_xml

Verwenden Sie den Befehl `devicelist_xml`, um ein XML-Dokument mit einer Liste aller Bestände und Monitore zu erhalten, auf die der Benutzer Zugriff hat.

Syntax

```
http://localhost/KNM/extract.xsi?cmd=devicelist_xml&user=Admin
```

cmd	devicelist_xml
user	KNM user username

Ausgegebene Daten

Ein XML-Dokument.

XML-Felder

DEVICELIST	Stamm der Baumstruktur
DEVICE	Stamm des Bestands
NAME	Name des Bestands
DESC	Beschreibung des Bestands
ID	ID des Bestands

MONITOR	Stamm des Bestands
ID	ID des Monitors
NAME	Name des Monitors

Beispiel

```
<DEVICELIST>
   <DEVICE>
           <NAME>Fileserver</NAME>
           <DESC>Office fileserver</DESC>
```

```
            <ID>955</ID>
                    <MONITOR>
                            <ID>8</ID>
                            <NAME>Bandwidth test</NAME>
                    </MONITOR>
   </DEVICE>
</DEVICELIST>
```

user_status

Verwenden Sie den Befehl `user_status`, um den Benutzerstatus und Benutzerinformationen zu erhalten.

Syntax

```
http://localhost/knm/extract.xsi?cmd=user_status&user=Admin&id=2
```

cmd	user_status
user	KNM user username
id	ID des Benutzers

Ausgegebene Daten

Eine Zeichenfolge, die den Benutzerstatus und Benutzerinformationen enthält; die Felder sind durch einen senkrechten Strich (|) voneinander getrennt.

Format der ausgegebenen Daten

```
UserName | Name | Phone | Cell phone | Address 1 | Address 2 | Scheduled status | Online status
```

Benutzername	KNM user username
Name	Tatsächlicher Name
Telefon	Telefonnummer
Mobiltelefon	Mobiltelefonnummer
Adresse 1	Adressfeld
Adresse 2	Adressfeld
Planmäßiger Status	"Available" (Verfügbar), falls der Benutzer eingeplant und im Dienst ist; "n/a" (Nicht verfügbar), falls der Benutzer nicht eingeplant oder nicht im Dienst ist
Online-Status	"Online", wenn der Benutzer in KNM angemeldet ist

Beispiel

```
Admin | Robert | 0611-22334 | | Box 277 | 871 31 Härnösand Sweden | n/a | Online
```

test_status

Verwenden Sie den Befehl `test_status`, um eine Übersicht über den Status aller Monitore zu erhalten.

Syntax

```
http://localhost/knm/extract.xsi?cmd=test_status&user=Admin
```

cmd	test_status
user	KNM user username

Ausgegebene Daten

Eine Zeichenfolge mit dem aktuellen Teststatus. Sie gibt Aufschluss darüber, ob ein oder mehrere Monitore den Status "Fehlgeschlagen" oder "Alarm" aufweisen.

Beispiel

```
ALARM
```

Version

Verwenden Sie den Befehl `version`, um die aktuelle **Network Monitor**-Versionsnummer zu erhalten.

Syntax

```
http://localhost/knm/extract.xsi?cmd=version&user=Admin
```

cmd	Version
user	KNM user username

Ausgegebene Daten

Eine Zeichenfolge mit der aktuellen Versionsnummer von **Network Monitor**.

Beispiel

```
7.0
```

UNIX-Systemunterstützungsdateien

Es hängt vom Systemtyp ab, welche Monitortypen für einen Bestand verfügbar sind und auf welche Art und Weise diese den Test durchführen.

Network Monitor unterstützt alle integrierten Windows-Systemtypen. Neue *Systemtypen* können mithilfe eines Konfigurationsdateisets erstellt werden, das sich im Ordner `KNM\system` des KNM-Hostrechners befindet.

> **Hinweis:** Der Fokus dieses Abschnitts liegt hauptsächlich auf UNIX; die Anweisungen können jedoch auf alle Systemtypen übertragen werden, die über einen Shellzugriff über SSH oder Telnet verfügen.

Systemspezifikationen

Um die Überwachung einer Disk, CPU, Auslagerungsdatei usw. zu ermöglichen, meldet **Network Monitor** sich mithilfe von SSH oder Telnet an, führt einen Befehl auf dem UNIX-Host aus und analysiert das Ergebnis. Welcher Befehl ausgeführt wird und wie das Ergebnis analysiert wird, ist in den Konfigurationsdateien im Ordner `KNM\system` beschrieben.

Alle Systemspezifikationen erben denjenigen, der mit `Generic UNIX` beschriftet ist. Es müssen also nur für diejenigen Befehle Analyseinformationen geschrieben werden, die sich von den Befehlen, die im Systemtyp `Generic UNIX` festgelegt sind, unterscheiden.

Generische UNIX-Systemdefinitionsdatei

```
<system name="Generic UNIX" release="" author="Kaseya" type="unix" internalID="5" fileRevision="1">
  <parsing>
    <!-- disk -->
    <disk>
      <!-- enumeration of disk volumes -->
      <enumeration>
        <query>
```

```
      <command>df</command>
      <enumList startLine="2">
        <value id="diskVolume" field="1" />
      </enumList>
    </query>
    <result id="volumeID">diskVolume</result>
  </enumeration>
  <!-- monitoring disk volumes-->
  <monitoring>
    <!-- free and used disk space -->
    <diskSpace>
      <query>
        <command>df -k $volume</command>
        <value id="freeSpace" line="-1" field="-3"/>
        <value id="usedSpace" line="-1" field="-4"/>
      </query>
      <result id="freeSpace" unit="MB">freeSpace / 1024</result>
      <result id="usedSpace" unit="MB">usedSpace / 1024</result>
    </diskSpace>
  </monitoring>
</disk>
<!-- cpu -->
<cpu>
  <!-- enumeration of CPU's -->
  <enumeration>
    <query>
      <command>mpstat -P ALL</command>
      <enumList startLine="5">
        <value id="cpuNumber" field="3" />
      </enumList>
    </query>
    <result id="cpuID">cpuNumber</result>
  </enumeration>
  <monitoring>
    <!-- utilization of given CPU-->
    <cpuUtilization>
      <query>
        <command>mpstat -P $cpu 2 2</command>
        <value id="userLoad" line="-1" field="-9"/>
        <value id="systemLoad" line="-1" field="-7"/>
      </query>
      <result id="cpuAverageLoad" unit="%">userLoad + systemLoad</result>
    </cpuUtilization>
    <!-- overall system CPU load, used if a CPU is not specified -->
    <cpuAverageLoad>
      <query>
        <command>vmstat 2 2</command>
        <value id="userLoad" line="-1" field="-5"/>
        <value id="systemLoad" line="-1" field="-4"/>
      </query>
      <result id="cpuAverageLoad" unit="%">userLoad + systemLoad</result>
    </cpuAverageLoad>
  </monitoring>
</cpu>
<!-- processes -->
<process>
  <!-- process enumeration -->
  <enumeration>
    <query>
      <command>ps -awxu</command>
      <enumList startLine="2">
        <value id="processName" field="11" />
      </enumList>
    </query>
    <result id="processName">processName</result>
  </enumeration>
  <monitoring>
    <!-- checks if a given process is running -->
    <processRunning>
```

```
        <query>
          <command>ps -awxu</command>
          <value id="processName">
            <match type="line">$process</match>
          </value>
        </query>
        <result id="processName">processName</result>
      </processRunning>
    </monitoring>
  </process>
  <!-- swap -->
  <swap>
    <monitoring>
      <swapUtilization>
        <query>
          <command>free -m</command>
          <value id="swapUsed" line="-1" field="-3"/>
          <value id="swapFree" line="-1" field="-2"/>
        </query>
        <result id="swapFree" unit="MB">swapFree</result>
        <result id="swapUsed" unit="MB">swapUsed</result>
      </swapUtilization>
    </monitoring>
  </swap>
  <!-- memory usage -->
  <memory>
    <monitoring>
      <!-- free and used memory -->
      <freeMemory>
        <query>
          <command>free -m</command>
          <value id="freeMem" line="3" field="-1"/>
          <value id="usedMem" line="3" field="-2"/>
        </query>
        <result id="freeMemory" unit="MB">freeMem</result>
        <result id="usedMemory" unit="MB">usedMem</result>
      </freeMemory>
    </monitoring>
  </memory>
  <!-- file change -->
  <file>
    <monitoring>
      <fileChange>
        <query>
          <command>ls -l --full-time $filename</command>
          <value id="fileSize" line="1" field="5"/>
          <value id="fileDate" line="1" field="6"/>
          <value id="fileTime" line="1" field="7"/>
        </query>
        <result id="fileSize" unit="B">fileSize</result>
        <result id="fileDate">fileDate</result>
        <result id="fileTime">fileTime</result>
      </fileChange>
    </monitoring>
  </file>
 </parsing>
</system>
```

Aktivierung des ODBC-Treibers

Mit der Aktivierung des ODBC-Treibers in der Standalone-Version des **Network Monitor** können Sie SQL-Anfragen auf die **Network Monitor**-Daten anwenden.

Voraussetzungen

- Stellen Sie sicher, dass "Microsoft Visual C++ 2010 Redistributable Package (x86)" und/oder "Microsoft Visual C++ 2010 Redistributable Package (x64)" auf der KNM-Hostmaschine installiert ist.

Installation

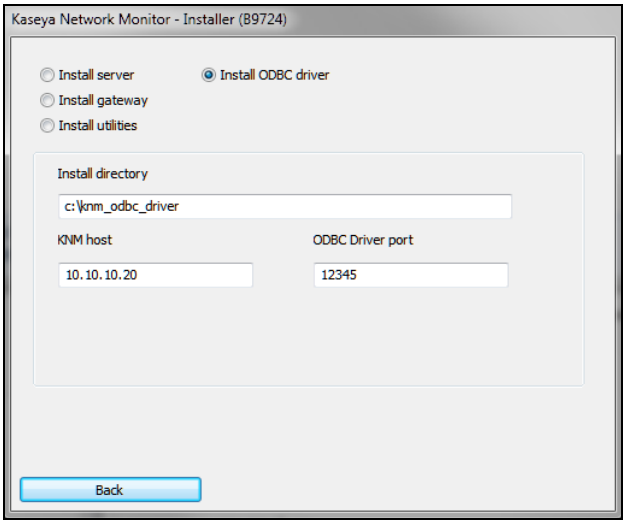
Auf VSA / Network Monitor-Server-Maschine

1. Öffnen Sie `cmd.exe` im Administrator-Modus.
2. Ändern Sie das Verzeichnis zum `knm`-Stammverzeichnis.
3. Ändern Sie das Verzeichnis zum `dsii_driver`-Verzeichnis unter dem `knm`-Stammverzeichnis.
4. Installieren Sie den KNM ODBC-Treiber mit folgendem Befehl:
   `dsii_driver.exe -Install`
5. Öffnen Sie den Service Control Manager und stellen Sie sicher, dass `"KNM5DSIIService"` gestartet ist und auf "automatischer" Start eingestellt ist.
6. Erstellen oder identifizieren Sie den **API-Schlüssel**, der mit jedem *beliebigen* **Network Monitor** Benutzer verknüpft ist. Dieses Feld befindet sich auf der Registerkarte Network Monitor > Benutzer > Eigene Einstellungen > **Registerkarte "Basiseigenschaften"** *(siehe 105)*.

   Hinweis: Geben Sie den **API-Schlüssel** als den Benutzernamen ein, der zur Authentifizierung verwendet wurde, als eine ODBC-Verbindung mit dem **Network Monitor**-Server hergestellt wurde. Das Authentifizierungspasswort kann eine beliebige Zeichenfolge sein.

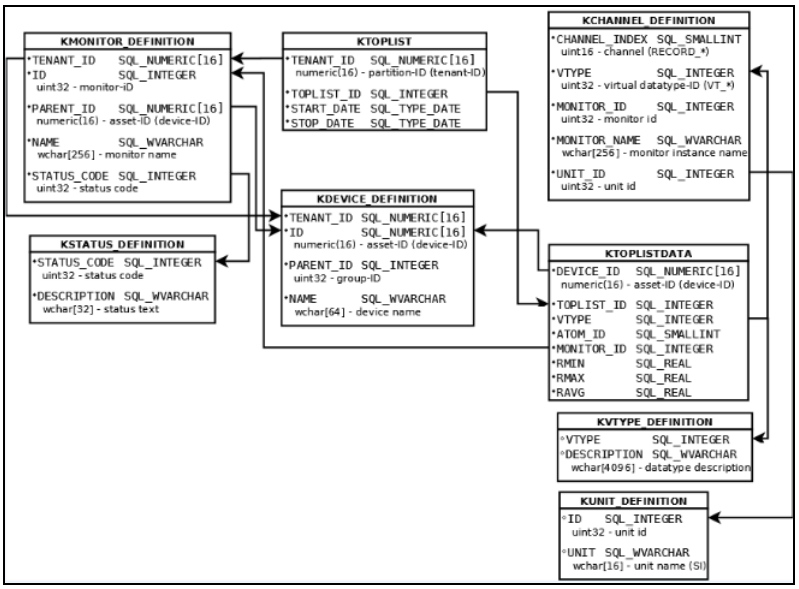
   Auf der lokalen Maschine

7. Kopieren Sie die `knmsetup.exe` Installationsdatei von <KaseyaInstallDirectory>\KNM\Installationsverzeichnis auf Ihre lokale Maschine.
8. Führen Sie `knmsetup.exe` auf Ihrer lokalen Maschine aus und wählen Sie die Option **ODBC-Treiber installieren**.
9. Geben Sie bei der Installation die IP-Nummer der KNM-Hostmaschine in das Feld "KNM-Host" ein und behalten Sie die Port-Nummer zum Standardport 12345 bei.



10. Ist die Installation abgeschlossen, sollten Abfragen der folgenden Tabellen möglich sein.
    `CHANNEL_DEFINITION`
    `ASSET_DEFINITION`
    `GROUP_DEFINITION`
    `MONITOR_DEFINITION`

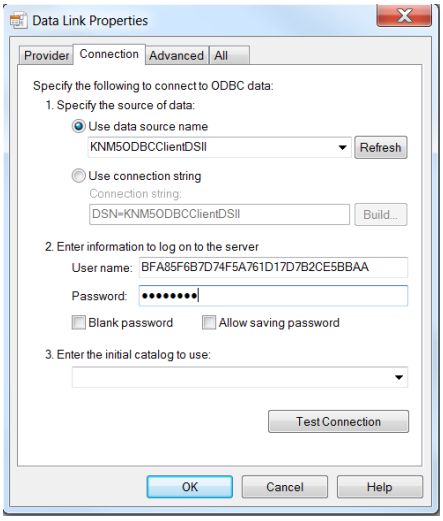
`STATUS_DEFINITION`
`UNIT_DEFINITION`
`VTYPE_DEFINITION`
`TOPLIST`
`TOPLISTDATA`



Beispiel: Abfragen von Network Monitor mithilfe von Excel 2010

1. Öffnen Sie ein leeres Arbeitsblatt in *Excel 2010*.
2. Wählen Sie die Option **Daten > Aus anderen Quellen > Vom Datenverbindungs-Assistenten**.
3. Wählen Sie die Option **ODBC DSN**.
4. Wählen Sie die **ODBC-Datenquelle** für **Network Monitor**. Standardmäßig lautet dieser Name `KNM50DBCClientDSII`.
5. Wählen Sie die folgenden Datenquelleneigenschaften.
   - **Datenquellenname verwenden** – `KNM50DBCClientDSII`
   - **Benutzername** – Geben Sie den **API-Schlüssel** für einen beliebigen Benutzer in Ihrem Network Monitor-Server an. Ein **API-Schlüssel** wird mithilfe von > Benutzer und Benutzergruppen > Erstellen Sie einen neuen Benutzer > **Registerkarte "Basiseigenschaften"** *(siehe 105)* erstellt oder identifiziert.

- **Passwort** – Geben Sie eine beliebige Zeichenfolge ein.



6. Wählen Sie die **Network Monitor**-Tabelle, zu der Sie eine Datenverbindung herstellen möchten.
7. Speichern Sie die Datenverbindungsdatei. Dadurch können Sie die Datenverbindung zu einem späteren Zeitpunkt erneut nutzen.
8. Wählen Sie aus, wie Sie die Daten und die Anfangszelle in Ihrer Arbeitsmappe anzeigen möchten.
9. Prüfen Sie den **Network Monitor**, der jetzt im Arbeitsblatt angezeigt wird.
10. Jetzt brauchen Sie nur noch auf **Aktualisieren** (Alt+F5) klicken, um die im Arbeitsblatt angezeigten **Network Monitor**-Daten zu aktualisieren.

Kapitel 6

Windows-Problembehandlung und -Systemmonitor

In diesem Kapitel

Fehlerbehebung – Windows-Überwachung und -authentifizierung 190
Windows-Leistungsregistrierung 194
Windows-Verwaltungsinstrumentation (WMI) 195

Fehlerbehebung – Windows-Überwachung und -authentifizierung

Network Monitor bietet die Möglichkeit, Windows-Arbeitsplatzrechner und -Dienste *ohne Agent* aus der Ferne (remote) zu überwachen. Voraussetzung für eine Remote-Überwachung ist die erfolgreiche Authentifizierung mit einem Windows-Account, der den Zugriff auf verschiedene Ressourcen innerhalb des überwachten Bestands ermöglicht.

Bei der Remote-Überwachung kann eine Reihe unterschiedlicher Probleme auftreten. Dieser Abschnitt beschäftigt sich mit denjenigen Problemen, die am häufigsten auftreten.

Warnung: Dieser Abschnitt dient lediglich als Referenz für die Fehlerbehebung; Kaseya kann keine Garantie dafür übernehmen, dass sich anhand der Erläuterungen in diesem Abschnitt alle auftretenden Probleme beheben lassen. Bitte beachten Sie, dass Sie für alle Änderungen, die Sie am System (einschließlich der Registry) vornehmen, selbst Verantwortung tragen.

Network Monitor -Dienstkonto und Zuweisung von Rechten

Wird der `Kaseya Network Monitor`-Dienst unter einem anderen Benutzerkonto als `LocalSystem` ausgeführt, müssen die folgenden lokalen Sicherheitsrichtlinien für das Dienstkonto aktiviert sein:

- Anmelden als Dienst
- Einsetzen als Teil des Betriebssystems (Windows 2000)
- Auslassen der durchsuchenden Überprüfung
- Lese- und Schreibzugriff sowie Ausführungsberechtigungen für den `KNM`-Ordner des KNM-Hostrechners.

Um die integrierte Kontenverwaltung in vollem Umfang nutzen zu können, sollten alle Bestände einem anderen Konto als dem Basisdienstkonto zugewiesen sein.

Überwachungskonten

Mit **Network Monitor** haben Sie die Möglichkeit, jedem Bestand ein Standardkonto zuzuweisen. Dieses Konto ermöglicht den Zugriff auf den überwachten Bestand.

Im Folgenden wird dieses Konto als *Überwachungskonto* bezeichnet. Auf der Seite **Bestand bearbeiten** *(siehe 47)* trägt dieses Konto den Namen **Standardkonto**. Auf der Seite Monitor bearbeiten sollte die Option zur Kontenauswahl auf **Standardkonto des Bestands verwenden** gesetzt sein.

Das Überwachungskonto sollte innerhalb des überwachten Bestands der Gruppe `Administrators` angehören. In den meisten Fällen handelt es sich dabei um die Gruppe `Domain Admin`.

Format des Konto-Benutzernamens

Je nach Standort des Überwachungskontos erfordert **Network Monitor** gegebenenfalls die Formatierung des Benutzernamens gemäß den folgenden Regeln. Diese Regeln gelten auch für Windows im Allgemeinen.

- `.\username` – Konto wird von **Network Monitor** auf dem lokalen Rechner gefunden.
- `username` – Konto wird von **Network Monitor** auf dem lokalen Rechner gefunden.
- `domain\username` – Konto wird von **Network Monitor** anhand des Domain-Namens gefunden.
- `username@domain.com` – Wie oben, gilt allerdings für Windows XP, 2003 und Vista.

Monitore mit Windows-Authentifizierung

Die folgenden Monitore erfordern alle eine Windows-Authentifizierung:

- `CPU utilization`
- `Disk utilization`
- `Memory utilization`
- `Swap file utilization`
- `Process`
- `Windows performance`
- `WMI`

Diese Monitore nutzen den Remoteregistrierungsdienst, um den überwachten Bestand abzufragen. Stellen Sie sicher, dass der Remoteregistrierungsdienst sowohl auf dem überwachten Bestand als auch auf dem **Network Monitor**-Host ausgeführt wird.

Standardmäßig können nur Administratoren auf die Remoteregistrierung zugreifen. Dies wird mithilfe des Registrierungsschlüssels geregelt.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg
```

Sie können die mit dem Registrierungsschlüssel verbundenen Berechtigungen bearbeiten, um den Zugriff auf die Remoteregistrierung zu gewähren oder zu beschränken. Gibt es diesen Schlüssel nicht, so hat jeder Zugriff auf die Remoteregistrierung.

Um einen Sonderfall handelt es sich beim Monitor `Disk utilization` im Kompatibilitätsmodus. In diesem Fall müssen Sie die Standardfreigabe angeben, die die überwachte Disk repräsentiert. So sollten Sie beispielsweise nicht `C:`, sondern `C$` angeben und sicherstellen, dass diese Standardfreigabe existiert und dass das Überwachungskonto darauf zugreifen kann.

Ereignisprotokollmonitor

Standardmäßig kann jeder das Ereignisprotokoll – mit Ausnahme des `Security`-Ereignisprotokolls – einsehen. Um das `Security`-Ereignisprotokoll einsehen zu können, muss der jeweilige Benutzer Mitglied der Administratorengruppe sein. Der Zugriff auf die verschiedenen Ereignisprotokolle wird durch den folgenden Registrierungsschlüssel geregelt:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog
```

Sie können die mit dem Registrierungsschlüssel verbundenen Berechtigungen bearbeiten, um den Zugriff auf das Remote-Ereignisprotokoll zu gewähren oder zu beschränken.

Dienstmonitor

Dieser Monitor nutzt den `Remote Procedure Call (RPC)`-Dienst, um den Status eines Dienstes abzufragen, der auf dem überwachten Rechner ausgeführt wird. Stellen Sie sicher, dass der `Remote Procedure Call (RPC)`-Dienst sowohl auf dem überwachten Bestand als auch auf dem **Network Monitor**-Host ausgeführt wird. Das Überwachungskonto muss mit Administratorrechten für den überwachten Host ausgestattet sein, um auf die Dienstverwaltung zugreifen zu können.

Externe Ressourcen

> **Warnung:** Die folgenden Verknüpfungen sind lediglich als Empfehlungen gedacht. Bitte beachten Sie, dass Sie für alle Änderungen, die Sie am System (einschließlich der Registry) vornehmen, selbst Verantwortung tragen.

- **So beschränken Sie den Zugriff auf die Registrierung von einem Remotecomputer aus** *(http://support.microsoft.com/kb/153183/en-us)*
- **Das Entfernen der Gruppe "Jeder" aus den Gruppenrichtlinien im Remoteregistrierungsdienst löscht dauerhaft alle Zugriffsrechte** *(http://support.microsoft.com/kb/281641/en-us)*

- **Ein benutzerdefiniertes Programm, das die Funktion "RegConnectRegistry" verwendet, kann in Windows Server 2003 mit Service-Pack 1 oder in einer x64-basierten Version von Windows Server 2003 nicht mehr auf die Registry eines Remote-Computers zugreifen** *(http://support.microsoft.com/kb/906570)*
- **Steuern des Systemmonitor-Remotezugriffs auf Windows NT-Server** *(http://support.microsoft.com/kb/164018/en-us)*
- **Problembehandlung bei Leistungsindikatoren** *(http://support.microsoft.com/kb/152513/en-us)*
- **Fehlermeldung "Vorgang auf <Ereignisprotokoll> konnte nicht abgeschlossen werden. Zugriff wurde verweigert." beim Versuch, sich an einem Windows Server 2003-basierten Computer anzumelden** *(http://support.microsoft.com/kb/888189/en-us)*
- **Fehlermeldung "Zugriff verweigert" beim Versuch, von einem Computer mit Windows Server 2003 und Service-Pack 1 aus eine Remote-Verbindung zur Registry eines Windows-basierten Computers herzustellen** *(http://support.microsoft.com/kb/913327/en-us)*

Fehlerbehebung

In diesem Abschnitt wird erläutert, wie einige der am häufigsten auftretenden Probleme mit der Windows-Authentifizierung behoben werden können.

Zugriff verweigert

Tritt bei der Überwachung eines Bestands entweder als spontaner oder als dauerhafter Fehler auf.

```
Access denied.
```

Anlass

Der Zugriff auf den überwachten Bestand wurde verweigert. Die Ursache hierfür kann sein, dass ein Authentifizierungsfehler vorliegt oder dass der überwachte Bestand zu beschäftigt mit der Übermittlung neuer Anforderungen ist.

Lösung/Umgehung des Problems

- Stellen Sie sicher, dass das Überwachungskonto mit Zugriffsrechten für den überwachten Bestand ausgestattet ist. Meistens wird dieser Fehler dadurch ausgelöst, dass das **Network Monitor**-Überwachungskonto nicht mit Administratorrechten für den überwachten Bestand ausgestattet ist.
- Verlängern Sie das Testintervall des Monitors.
- Nutzen Sie die **Alarmfilterungsfunktionen** des Monitors, um Fehler herauszufiltern, die nicht mit dem Schwellenwert zusammenhängen.
- Einschränkungen durch die Firewall hindern **Network Monitor** daran, auf den überwachten Bestand zuzugreifen. Dieser Fehler kann behoben werden, indem die Blockierung von Port 445 für den überwachten Bestand aufgehoben wird.

Netzwerkpfad kann nicht gefunden werden

Tritt bei der Überwachung eines Bestands entweder als spontaner oder als dauerhafter Fehler auf.

```
The network path was not found.
```

Anlass

Aufgrund von Firewallbeschränkungen, eines Fehlers bei der Namensauflösung oder eines Netzwerkfehlers konnte der Netzwerkpfad nicht gefunden werden bzw. nicht auf den Netzwerkpfad zugegriffen werden.

Lösung/Umgehung des Problems

- Der DNS-Server ist überlastet und kann die Bestandsadresse nicht übersetzen. Versuchen Sie, die IP-Adresse als Bestandsadresse einzugeben.

- Einschränkungen durch die Firewall hindern **Network Monitor** daran, auf den überwachten Bestand zuzugreifen. Dieser Fehler kann behoben werden, indem die Blockierung von Port 445 für den überwachten Bestand aufgehoben wird.
- Falls es sich beim Monitor um einen `Disk utilization`-Monitor handelt und Sie diesen im Win32-Kompatibilitätsmodus ausführen, stellen Sie sicher, dass die Freigabe verfügbar ist. Wenn Sie lieber direkt eine Disk anstatt einer Freigabe überwachen möchten, verwenden Sie den Standardfreigabenamen der Disk (z. B. `C$`) anstatt des Datenträgernamens (z. B. `C:`).

Leistungsprobleme bei überwachten Beständen

Es treten spontane Fehler zu einer bestimmten Tageszeit oder auch in anderen Mustern auf, so zum Beispiel zu Beginn einer Sicherung oder bei der Ausführung umfangreicher Abfragen einer Datenbank im überwachten Bestand.

Anlass

Der überwachte Bestand ist möglicherweise nicht in der Lage, Anforderungen von **Network Monitor** abzuschließen, weil er mit anderen Aufgaben beschäftigt ist. Das Problem kann auch mit der Bandbreite des Netzwerks zusammenhängen. So kann beispielsweise die Überwachung von Beständen über eine VPN-Verbindung die Netzwerkleistung und -latenz schwer beeinträchtigen. Es können verschiedene Fehlermeldungen vorkommen; die meisten stehen jedoch mit RPC-Fehlern in Zusammenhang.

Lösung/Umgehung des Problems

- Setzen Sie die Testfrequenz auf 300 Sekunden herab.
- Setzen Sie den Wert für die **Alarmerzeugung** auf mindestens 5, um falsch positive Ergebnisse herauszufiltern.
- Nutzen Sie die **Alarmfilterungsfunktionen** des Monitors, um Fehler herauszufiltern, die nicht mit dem Schwellenwert zusammenhängen.
- Sollten eine geringe Netzwerkbandbreite oder eine hohe Netzwerklatenz eine Rolle spielen, kann ein Gateway näher am überwachten Bestand platziert werden. Ein Gateway beansprucht nur einen Bruchteil der Netzwerkbandbreite, die ein normaler Test in Anspruch nimmt.

Der RPC-Server ist nicht verfügbar

Es treten entweder von Zeit zu Zeit oder auch ständig Fehler mit dem folgenden Fehlertext auf:

```
The RPC server is unavailable
```

Anlass

Meistens besteht die Ursache dieses Problems darin, dass die Remoteregistrierung des überwachten Rechners entweder beendet wurde oder Probleme beim Annehmen neuer Verbindungen aufgetreten sind.

Lösung/Umgehung des Problems

- Starten Sie den Remoteregistrierungsdienst des überwachten Bestands neu.
- Überprüfen Sie die Gesamtleistung des Bestands. Möglicherweise ist der Bestand mit der Übermittlung immer neuer Verbindungen überlastet.
- Nutzen Sie die Alarmfilterungsfunktionen des Monitors, um Fehler herauszufiltern, die nicht mit dem Schwellenwert zusammenhängen.
- Prüfen Sie den DNS-Eintrag für den überwachten Bestand und stellen Sie sicher, dass sowohl ein Eintrag für die Forwardzone als auch für die Reversezone existiert.

Windows-Leistungsregistrierung

Das Windows-Leistungsregister ist eine virtuelle Registrierungsstruktur, die Leistungsmetriken von mehreren installierten Providern enthält. Sämtliche Kommunikation mit der Leistungsregistrierung geschieht über den Remoteregistrierungsdienst

Die folgenden Monitore können die Windows-Leistungsregistrierung verwenden

- Windows-Systemmonitor
- CPU-Monitor
- Speichermonitor
- Größenauslagerungsmonitor
- Bandbreitenmonitor
- Datenträgermonitor

Alle Monitore außer dem Windows-Systemmonitor können zur Verwendung von WMI gezwungen werden, indem das Kontrollkästchen **WMI verwenden** auf der Seite **Bestandseigenschaft** markiert wird.

Advanced properties (Click to expand/hide)
Simple maintenance:
Day of week:
Mon Tue Wed Thu Fri Sat Sun
Time zone:
GMT +1
Root monitor:
SNMP port:
161
Favourite:
No SSH2 con. sharing:
No inspection:
Use WMI:
Wake-On-LAN:
Specify maintenance period for this object here in HH:MM format. This period can wrap to the next day if needed.
Select which day(s) of the the week the maintenance schedule will be active.
Time zone where object is located. Selecting a timezone will cause realtime charts in this object to be displayed in the object's local time.
Root monitor in a local dependency tree. Select the monitor which all other monitors in this object will be dependent on. If this is a template, the dependency tree will be inherited.
Connection port for SNMP communication.
Tag as a favourite.
Disable the use of persistent SSH2 connections for this object.
Disable automatic object inspection on this object.
Use WMI for performance monitoring on this object.
If you want to specify actions to send Wake-On-LAN packets to this machine, specify the MAC-address of the interface you wish to send those packets to here. Format is AA-BB-CC-DD-EE-FF.

Unterthemen

- **So überprüfen Sie, ob KNM Zugriff auf den Remoteregistrierungsdienst hat** *(siehe 194)*
- **Arbeitsspeicherverlust bei Remoteregistrierungsdienst auf überwachtem Rechner** *(siehe 195)*
- **Zwischenspeichern von Zählern** *(siehe 195)*

So überprüfen Sie, ob KNM Zugriff auf den Remoteregistrierungsdienst hat

1. Melden Sie sich auf dem KNM-Hostrechner mit dem Windows-Konto an, das zum Monitoring verwendet wird
2. Starten Sie die 32-Bit-Version der `perfmon.exe`-Anwendung. Diese Datei befindet sich auf einem 64-Bit-Rechner im Verzeichnis `SysWOW64`.
3. Melden Sie sich auf dem überwachten Rechner an und fügen Sie einen Zähler hinzu.

Wenn der Test fehlschlägt, kann **Network Monitor** die Zähler auf dem überwachten Rechner nicht aufzählen und Proben entnehmen.

1. Prüfen Sie, ob die Firewall zur Remote-Verwaltung im korrekten Profil geöffnet ist.
2. Stellen Sie sicher, dass der Remoteregistrierungsdienst auf dem überwachten Rechner ausgeführt wird.
3. Überprüfen Sie, ob das Konto auf die Leistungsindikatorstruktur zugreifen darf. Siehe **http://support.microsoft.com/kb/300702/en-us** *(http://support.microsoft.com/kb/300702/en-us)*.
4. Wenn es sich um einen Standalone-Rechner mit Windows Vista/7 handelt (nicht um eine Domain), müssen Sie UAC deaktivieren, damit es nicht die Anmeldedaten herausfiltert. Siehe **http://support.microsoft.com/kb/951016** *(http://support.microsoft.com/kb/951016)*.

5. Wenn Zähler fehlen und Sie überprüft haben, dass die gleichen Zähler im `performon.exe`-Werkzeug fehlen, muss die Leistungsindikatorbibliothek eventuell neu aufgebaut werden. Siehe **http://support.microsoft.com/kb/300956** *(http://support.microsoft.com/kb/300956)*.
6. Wenn die Zähler immer noch fehlen, werden sie eventuell von einer dll-Datei mit 64-Bit veröffentlich; **Network Monitor** ist eine 32-Bit-Anwendung und kann noch keine 64-Bit-Zählerwerte lesen. Benutzer müssen entweder eine 32-Bit-Version der dll-Datei installieren oder den Zähler mit WMI abfragen.

Arbeitsspeicherverlust bei Remoteregistrierungsdienst auf überwachtem Rechner

Da die Leistungsregistrierungsstruktur externen ausführbaren Code lädt, um Leistungsdaten für Verbraucher zu veröffentlichen, z. B. **Network Monitor**, kann es zu Problemen mit den Modulen kommen, die geladen werden können, zum Beispiel zu Arbeitsspeicherverlust und Sperren.

Dies kann zu schlechten Speicherbedingungen auf dem überwachten Rechner führen.

Da eine Reparatur der problematischen dll-Dateien für uns nicht möglich ist, können wir – außer nach einer neueren Programmversion zu suchen – dem Benutzer nur empfehlen, ein geplantes Ereignis zu erstellen, das den Remoteregistrierungsdienst auf dem überwachten Rechner alle 24 Stunden neu startet.

Zwischenspeichern von Zählern

Wenn der Monitor eines Bestands seinen ersten Test nach dem Neustart durchführt, speichert er alle Zähler und [Winperf]-Bestandsnamen zwischen, um die Bandbreitenauslastung für alle folgenden Tests zu verbessern, die auf dem Bestand ausgeführt werden.

Dies kann ein Problem darstellen, wenn der Benutzer neue Software auf dem überwachten Rechner installiert, die zusätzliche Leistungsindikatoren veröffentlicht, nachdem **Network Monitor** mit einem Windows-Systemmonitor einen Test ausgeführt hat. Das Problem stellt sich als "fehlende Zähler" dar, wenn **Network Monitor** die Zähler aufzählt, aber sie im `perfmon.exe` -Werkzeug sichtbar sind.

Um den Cache zurückzusetzen, muss der Benutzer die **Network Monitor Systemadministratorkonsole** im Menü **Werkzeuge** öffnen. Der Benutzer muss Systemadministrator sein, um den Menüeintrag angezeigt zu bekommen. Geben Sie den folgenden Befehl ein:

```
clear-counter-cache <asset>
```

OBJECT_NAME ist der genaue Name des Bestands, dessen Cache zurückgesetzt wird.

Windows-Verwaltungsinstrumentation (WMI)

WMI wird standardmäßig bei allen Windows-Systemmonitoren verwendet, wenn ein neuer Bestand erstellt wird. Das WMI-Protokoll hat gegenüber älteren Windows-Leistungsregistrierungsaufrufen den Vorteil, dass es die Bandbreite effektiver nutzt. Auf manchen Plattformen, wie z. B. Windows Vista und Windows 2008 (ohne Service-Packs) beeinträchtigt WMI die Leistung stark und bei Überwachung dieser beiden Plattformen sollte deshalb Winperf vorgezogen werden.

Es ist bekannt, dass es für Systemadministratoren ohne Erfahrung schwierig ist, WMI für Remote-Monitoring zu konfigurieren.

WMI-Fehlerbehebung

Dieser Artikel beschreibt häufige Probleme bei der Windows-Systemüberwachung und wie sie behoben werden.

Hintergrund

Die folgende Fehlermeldung wird angezeigt

```
Access denied. User may lack remote launch and remote activation permission.
```

Die folgenden Monitortypen verwenden WMI, wenn die Bestandsmarkierung **WMI verwenden** aktiviert ist.

- WMI-Abfragemonitor (*)
- Active Directory-Monitor (*)
- Bandbreitenmonitor
- CPU-Monitor
- Datenträgermonitor
- Speichermonitor
- Auslagerungsmonitor

* Immer WMI verwenden

Diese Fehlermeldung wird angezeigt wenn:

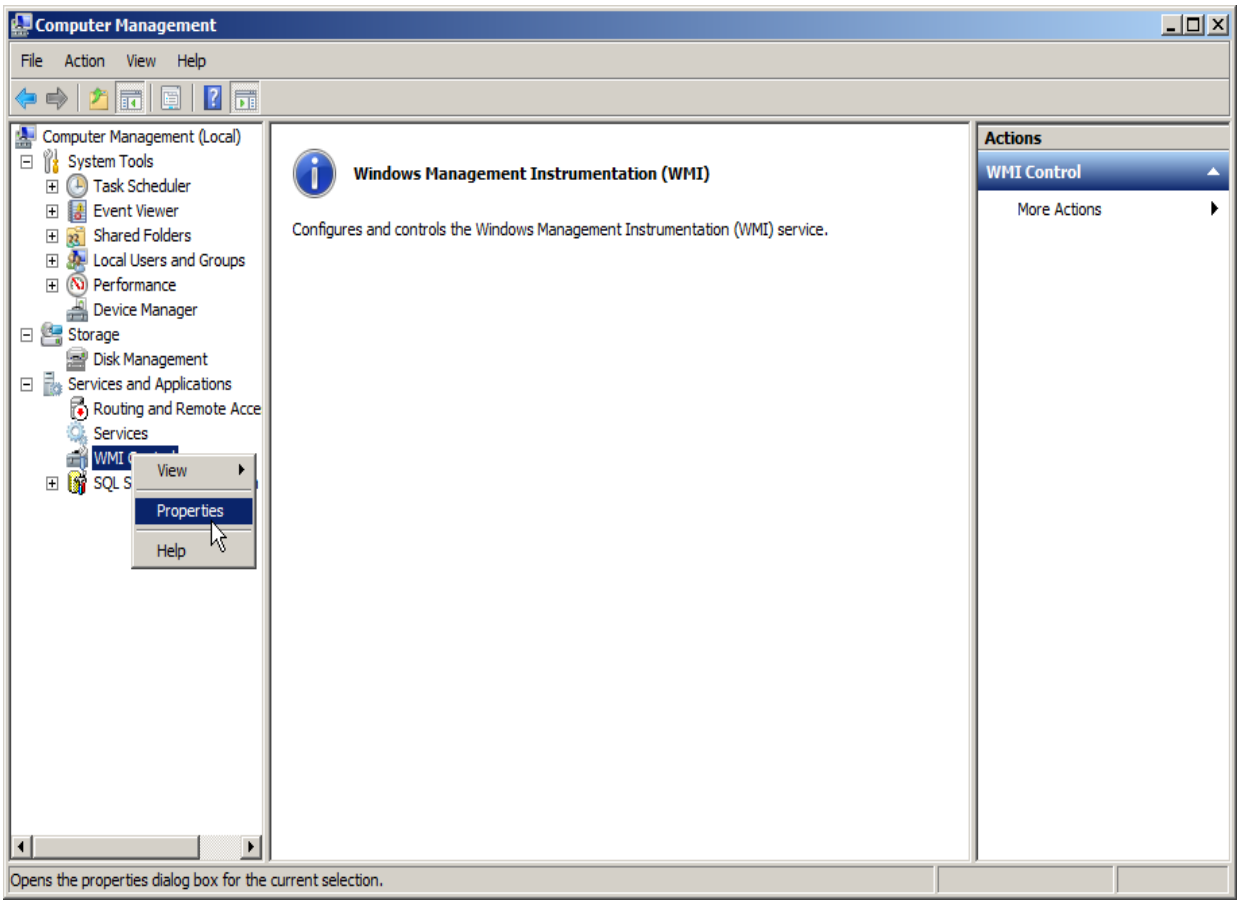
- das verwendete Benutzerkonto nicht dafür aktiviert ist, WMI in der Domain oder auf dem überwachten Rechner zu verwenden.
- die Firewall geschlossen ist.
- der Benutzer kein Administrator auf dem überwachten Rechner ist.

Unterthemen

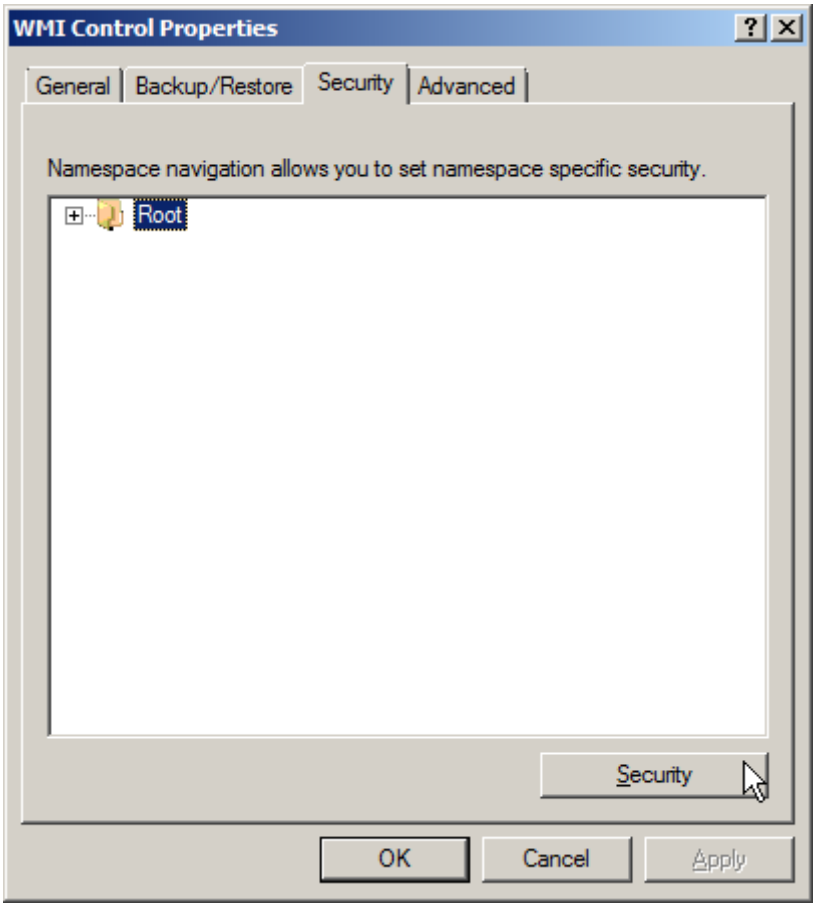
- **Überprüfen, ob WMI für das Konto aktiviert ist** *(siehe 197)*
- **Anpassen der Firewall-Einstellungen** *(siehe 199)*
- **Zusatz für Benutzer, die nicht Administrator sind** *(siehe 199)*
- **Überprüfen, ob WMI funktioniert** *(siehe 199)*
- Probleme mit zurückgegebenen Daten von Leistungsindikatoren, die von WMI gelesen werden
- **Vollständiger Index von Artikeln zur Fehlerbehebung bei Microsoft WMI** *(siehe 201)*

Überprüfen, ob WMI für das Konto aktiviert ist

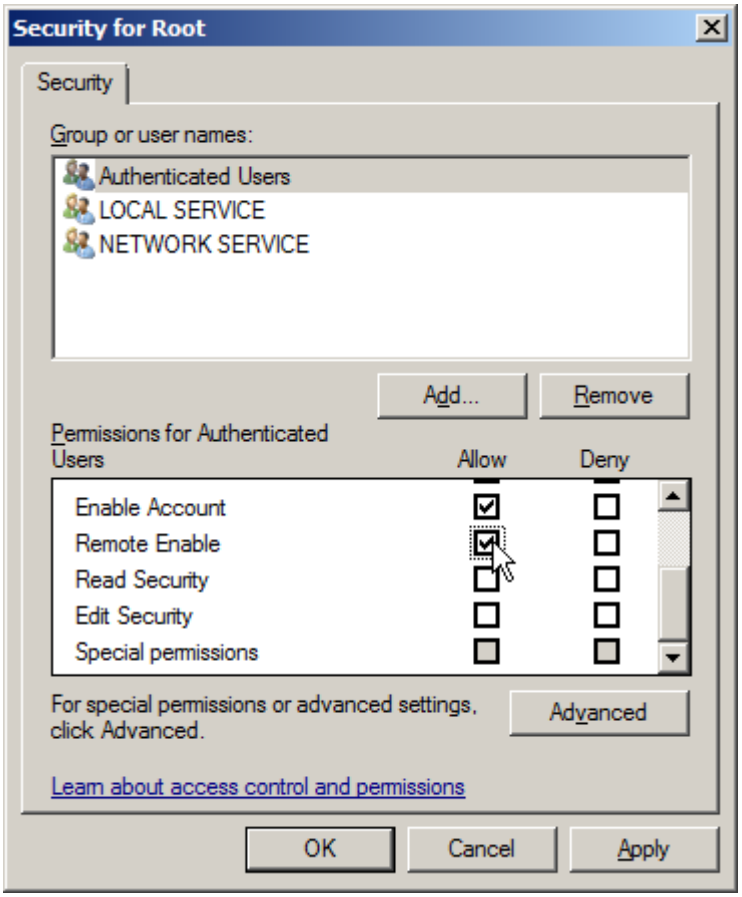
Öffnen Sie "Verwaltung" > Computer-Management und klicken Sie mit der rechten Maustaste auf "WMI-Steuerung", um die Option "Eigenschaften" auszuwählen.



Wählen Sie die Sicherheitsregisterkarte und klicken Sie auf "Sicherheit".



Aktivieren Sie "Remote aktivieren" für die Gruppe/den Benutzer, den Sie verwenden möchten.



Klicken Sie auf "Anwenden" und schließen Sie den Dialog.

Anpassen der Firewall-Einstellungen

Öffnen Sie die Eingabeaufforderung als Administrator und führen Sie den folgenden Befehl aus, um die eingehende Regel für WMI zu aktivieren.

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)"
new enable=yes
```

Zusatz für Benutzer, die nicht Administrator sind

Aktivieren Sie mit den einfachen Schritten im folgenden MSDN-Artikel den Benutzer, der nicht Administrator ist, dazu, mit DCOM zu interagieren.

- **http://msdn2.microsoft.com/en-us/library/Aa393266.aspx**
  (http://msdn.microsoft.com/en-us/library/aa393266.aspx)

Führen Sie im Artikel die Schritte aus, um:

- einem Benutzer oder einer Untergruppe einen DCOM-Remote-Start und Aktivierungsberechtigungen zu gewähren.
- DCOM-Remote-Zugriffsberechtigungen zu gewähren.

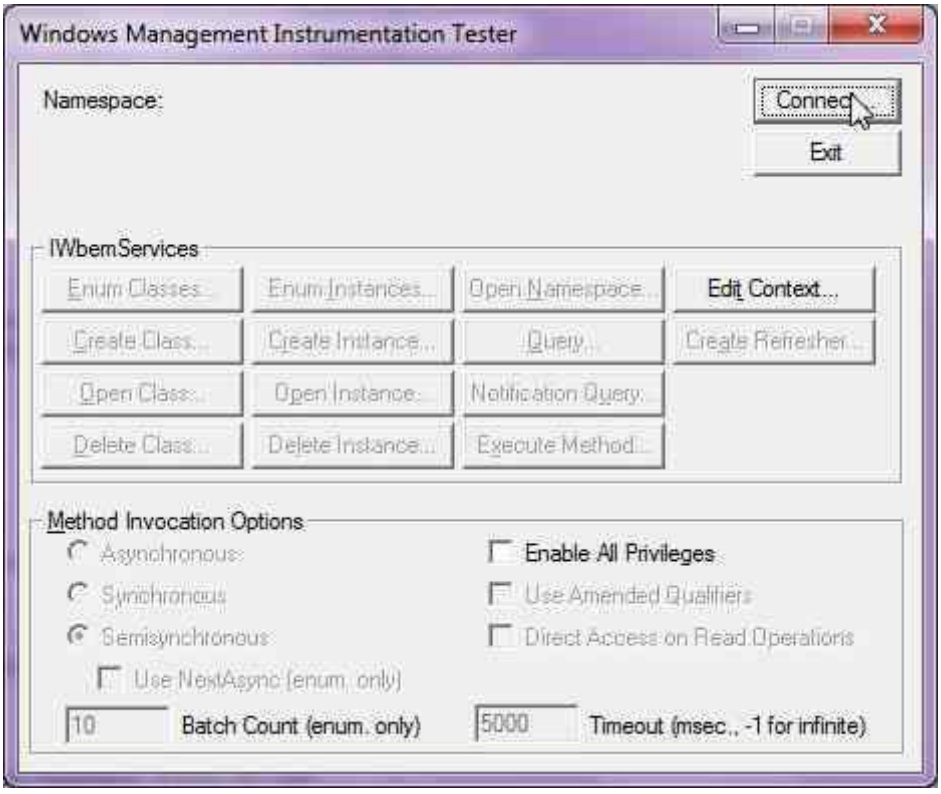
Überprüfen, ob WMI funktioniert

Das `wbemtest.exe`-Dienstprogramm kann verwendet werden, um zu prüfen, ob ein WMI-Aufruf vom KNM-Hostrechner zum überwachten Rechner gemacht werden kann. Zum Starten des Dienstprogramms melden Sie sich auf dem Desktop des KNM-Hostrechners an und öffnen Sie das

Startmenü. Geben Sie in das Feld "Ausführen" folgenden Text ein und drücken Sie Eingabe:

```
wbemtest.exe
```

Wenn das Dienstprogramm gestartet ist, klicken Sie auf die Schaltfläche "Verbinden".

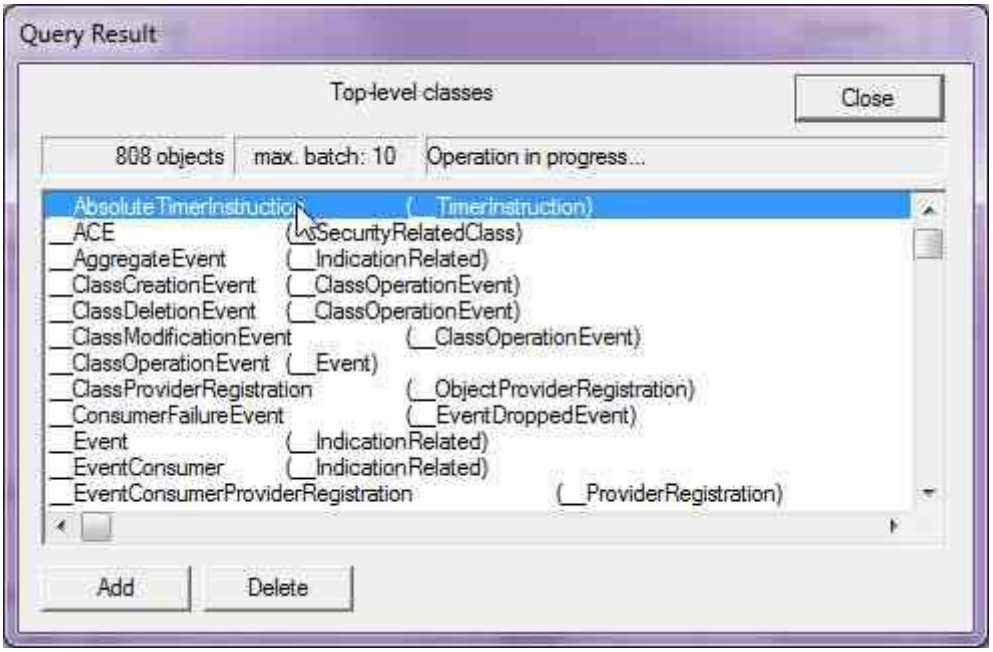


Geben Sie die folgende Adresse ein und ersetzen Sie "my_ip" mit der IP-Adresse des überwachten Rechners.

```
\\my_ip\root\cimv2
```

Geben Sie den Benutzernamen und das Kennwort ein, das Sie in KNM verwenden. Geben Sie in das Feld "Autorität" den Domain-Name des Benutzers ein. Klicken Sie auf "Verbinden" und dann auf "Klassen aufzählen".

Klicken Sie im Dialog "Info zu übergeordneter Klasse" auf das rekursive Optionsfeld und dann auf OK.



Das Dienstprogramm bestückt jetzt das Abfrageergebnisfenster mit Informationen vom überwachten Rechner. Wenn dies nicht geschieht, ziehen Sie die folgenden Informationen zur Fehlerbehebung auf der Microsoft Support-Website zu Rate.

Probleme mit zurückgegebenen Daten von Leistungsindikatoren, die von WMI gelesen werden

Manchmal funktioniert die Synchronisierung von Leistungsregister und WMI nicht oder der Prozess, der Leistungsdaten für WMI sammelt, kann auf einer gesperrten Ressource hängen bleiben.

Als letzte Möglichkeit nach Neustart des überwachten Rechners synchronisieren Sie die Leistungsindikatoren auf WMI mithilfe der in diesem Artikel aufgeführten Schritte.

- **http://support.microsoft.com/kb/266416** *(http://support.microsoft.com/kb/266416)*

Vollständiger Index von Artikeln zur Fehlerbehebung bei Microsoft WMI

- **http://msdn.microsoft.com/en-us/library/msaspx** *(http://msdn.microsoft.com/en-us/library/ms735120.aspx)*
- **http://msdn.microsoft.com/en-us/library/aa394603.aspx** *(http://msdn.microsoft.com/en-us/library/aa394603.aspx)*
- **http://msdn.microsoft.com/en-us/libraryAa393266.aspx** *(http://msdn.microsoft.com/en-us/library/aa393266.aspx)*
- **http://support.microsoft.com/kb/266416** *(http://support.microsoft.com/kb/266416)*
- **http://support.microsoft.com/kb/300956** *(http://support.microsoft.com/kb/300956)*
- **http://support.microsoft.com/kb/300702/en-us** *(http://support.microsoft.com/kb/300702/en-us)*
- **http://social.technet.microsoft.com/Forums/windows/en-US/8ed26d46-9994-4052-a307-5b071805aea8/wmi-corrupt-how-to-reinstallrepair**
  (https://social.technet.microsoft.com/Forums/windows/en-US/8ed26d46-9994-4052-a307-5b071805aea8/wmi-corrupt-how-to-reinstallrepair)
- **http://support.microsoft.com/kb/951016** *(http://support.microsoft.com/kb/951016)*

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

©2014 Kaseya. All rights reserved. | www.kaseya.com

Kapitel 7

Informationen zu Dienstprogrammen

In diesem Kapitel

Überblick über Dienstprogramme....204
Kompilieren von benutzerdefinierten MIB-Dateien....204
Lua....205
Gizmo....207
Dashboard Map Editor....208

Überblick über Dienstprogramme

Es werden vier weitere Dienstprogramme installiert, wenn Sie **Network Monitor** installieren. Diese Dienstprogramme müssen nicht **Network Monitor** verwenden. Sie befinden sich auf der Seite Network Monitor > Werkzeuge > **Downloads Dienstprogramme**

- **DME** – **Dashboard Map Editor** *(siehe 208)*.
- **Gizmo** – Die Anwendung **Gizmo** *(siehe 207)* für den Systeminformationsbereich.
- **MIB-Compiler** – Das **MIB-Compiler** *(siehe 99)*-Dienstprogramm.
- **Lua IDE** – Die **Lua** *(siehe 205)*-Entwicklungsumgebung

Kompilieren von benutzerdefinierten MIB-Dateien

Sie können MIB-Dateien mit MIB-Compiler in ein binäres Format kompilieren, das **Network Monitor** lesen kann. Für das Kompilieren von MIB-Dateien ist ein Wissen über die Funktionsweise von MIB-Dateien sowie ein generelles Verständnis von SNMP und **MIB-Objekten** *(siehe 98)* erforderlich. Eine Anzahl verschiedener RFC-Dokumente stellen die Grundlage, auf der alle anderen MIB-Dateien basieren, dar.

Hinweis: Der Communityname (SNMP-Version) und Port, der von **Network Monitor** verwendet wird, um eine Verbindung mit einem SNMP-Bestand zu erstellen, wird in der Registerkarte **Authentifizierung** *(siehe 40)* eines Bestandsknotens festgelegt. Der Bestandsknoten kann diese Einstellung von einem übergeordneten Knoten erben. Siehe **Installationscheckliste** *(siehe 4)*

Hierbei handelt es sich beispielsweise um die Kompilierungsreihenfolge des MIB eines CISCO®-Produkts.

1. `SNMPv2-SMI.mib`
2. `SNMPv2-TC.mib`
3. `SNMPv2-MIB.mib`
4. `RFC1213-MIB.mib`
5. `IF-MIB.mib`
6. `CISCO-SMI.mib`
7. `CISCO-PRODUCTS-MIB.mib`
8. `CISCO-TC.mib`

Die ersten fünf Dateien in diesem Beispiel sind für die meisten MiB-Dateien von Produkten einheitlich und werden in die standardmäßige binäre MIB-Datei `knm.mib` eingeschlossen.

Warnung: Alle diese Dateien müssen gleichzeitig kompiliert werden, andernfalls schlägt der MIB-Compiler aufgrund ungelöster Symbole fehl.

Inhalt der standardmäßigen MIB-Datei von KNM

Die Standarddatei `knm.mib`, die in der Installation eingeschlossen ist, enthält die folgenden Basis OIDs (Objektbezeichner).

- `iso.org.dod.internet.directory`
- `iso.org.dod.internet.mgmt`

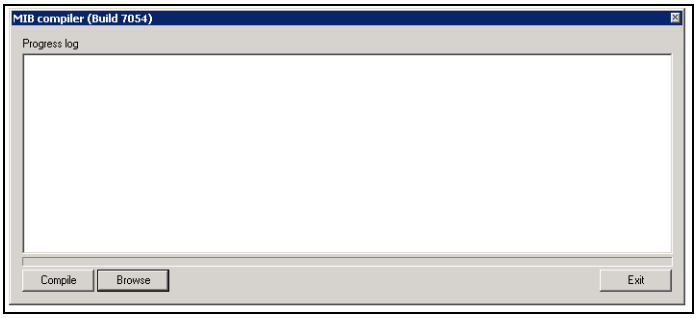
- `iso.org.dod.internet.experimental`
- `iso.org.dod.internet.private`
- `iso.org.dod.internet.security`

Die Datei befindet sich im Verzeichnis `\<KaseyaInstallDirectory>\KNM\mibs`.

Herunterladen und Ausführen des MIB-Compilers

1. Navigieren Sie zur Seite Network Monitor > Werkzeuge > **Downloads Dienstprogramme**.
2. Klicken Sie auf den Link des **MIB-Compilers**, um das Dienstprogramm auf den lokalen Rechner herunterzuladen.
3. Führen Sie das Dienstprogramm aus.

Kompilieren einer MIB-Datei



1. Starten Sie `<KaseyaInstallDirectory>\knm\mibcompiler.exe`.
2. Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine oder mehrere `*.mib` Dateien auszuwählen.
   - Suchen Sie die standardmäßige `knm.mib` Datei im `KNM\mibs`-Ordner des **Network Monitor**-Hostrechners. Doppelklicken Sie auf den Ordner, um ihn auszuwählen.
   - Wählen Sie alle zusätzlichen `*.mib` Dateien aus, die Sie in die Kompilierung einschließen möchten.
3. Klicken Sie auf die Schaltfläche **Kompilieren**.
4. Legen Sie fest, wo die kompilierte `*.dat` Datei gespeichert wird.
5. Klicken Sie auf die Schaltfläche **Durchsuchen**, um die `*.dat` Datei auszuwählen, die soeben kompiliert wurde. Eine interaktive MIB-Baumstruktur erscheint im Hauptfenster. Sie können diese verwenden, um zwischen den verschiedenen OIDs zu navigieren.
6. Verschieben oder kopieren Sie die kompilierte `*.dat` Datei in den Ordner `KNM\mibs`.

Lua

Lua ist eine leistungsfähige, schlanke Programmiersprache, die zur Erweiterung von Anwendungen entwickelt wurde. Lua wird außerdem häufig als eigenständige Mehrzwecksprache verwendet. Lua ist eine frei erhältliche Software. Lua verbindet einfache prozedurale Syntax mit leistungsfähigen Datenbeschreibungskonstrukten, die auf assoziativen Arrays und erweiterbarer Semantik basieren. Lua ist dynamisch typisiert, wird in Bytecodes übersetzt und verfügt über automatische Speicherverwaltung mit automatischer Speicherbereinigung, wodurch sie ideal für Konfiguration, Skripting und Rapid Prototyping ist.

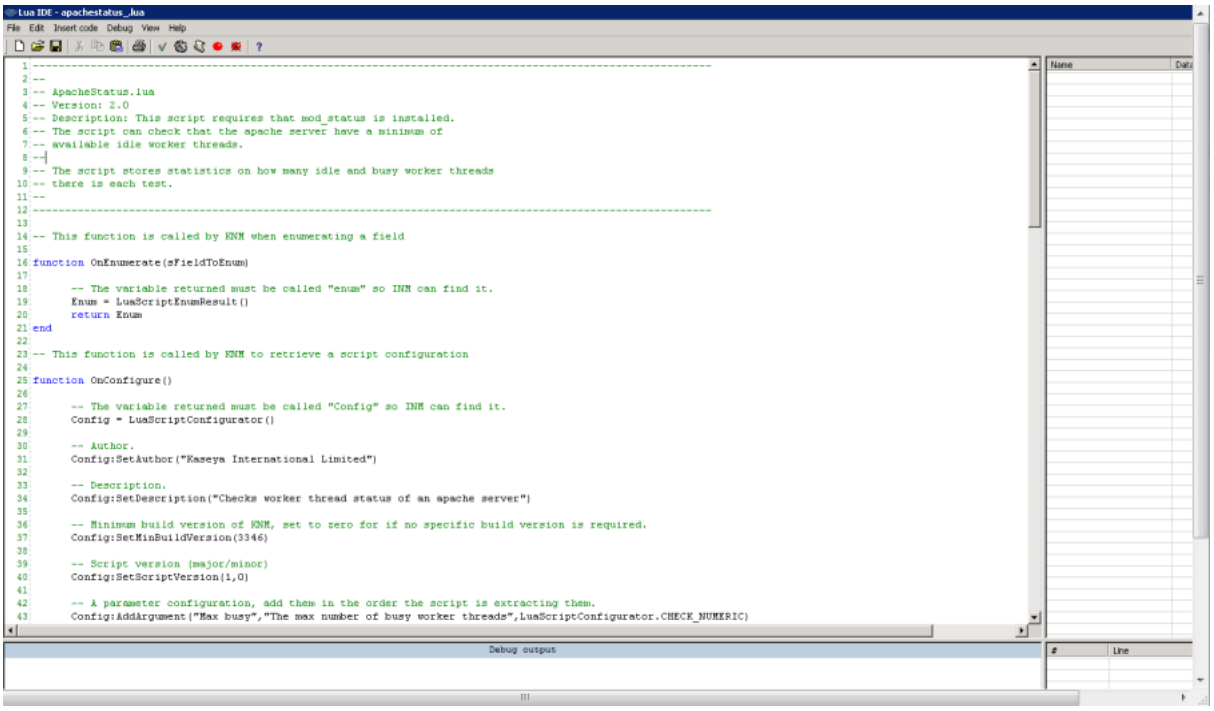
Network Monitor und Lua

Network Monitor unterstützt die Skriptsprache Lua (`www.lua.org`).

- Kunden können benutzerdefinierte Monitore erstellen, um Systeme und Arbeitsgeräte zu testen, die von einer aktuell verwendeten Monitoringlösung nicht unterstützt werden.

- Neue Monitore, Aktionen und Ereignisse können in der von Kaseya zur Verfügung gestellten Entwicklungsumgebung erstellt und getestet werden, bevor sie in **Network Monitor** exportiert und verwendet werden.
- Den Entwicklern steht eine umfassende Bibliothek vordefinierter Klassen, wie z. B. FTP-Clients, HTTP-Clients und Dateiverwaltung zur Verfügung. Siehe **KNM API-Dokumentation** *(http://help.kaseya.com/webhelp/DE/knm/R8/api/index.asp#home.htm)* für weitere Informationen zu verschiedenen vordefinierten Klassen.

Die Entwicklungsumgebung beinhaltet Debugger, Hervorhebung von Schlüsselwörtern, eine integrierte Hilfe und andere Funktionen, die in modernen Entwicklungstools verfügbar sind.



Herunterladen und Ausführen von Lua IDE

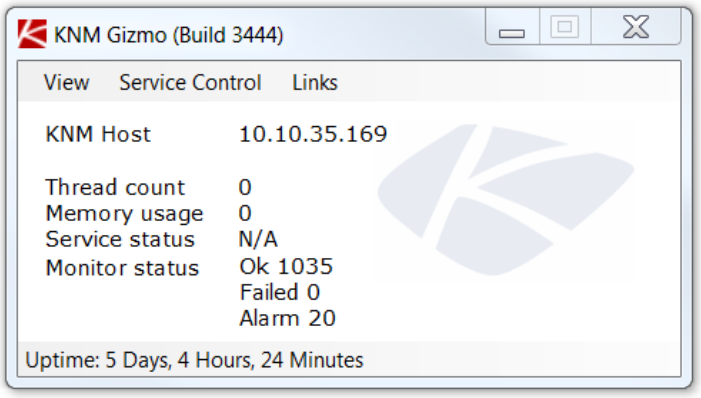
1. Navigieren Sie zur Seite Network Monitor > Werkzeuge > **Downloads Dienstprogramme**.
2. Klicken Sie auf den Link **Lua IDE**, um das Dienstprogramm auf den lokalen Rechner herunterzuladen.
3. Führen Sie das Dienstprogramm aus.

In KNM enthaltene Lua-Module

- Base
- Math
- String
- Tabelle

Gizmo

Gizmo ist eine kleine Anwendung für den Systeminformationsbereich, die Sie auf Ihrem Arbeitsplatzrechner installieren können.



Merkmale

- Alarmmitteilung
- Network Monitor Protokollanzeige
- Starten/Beenden von Network Monitor
- Statistiken, einschließlich der Speicherauslastung, CPU-Auslastung und Betriebszeit von Network Monitor.

Anforderungen

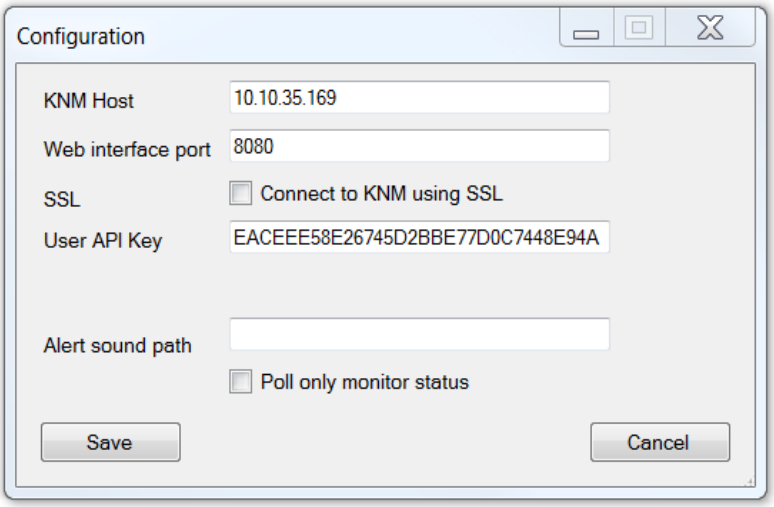
- Net 2.0 Runtime installiert

Herunterladen und Ausführen von Gizmo

1. Navigieren Sie zur Seite Network Monitor > Werkzeuge > **Downloads Dienstprogramme**.
2. Klicken Sie auf den Link **Gizmo**, um das Dienstprogramm auf den lokalen Rechner herunterzuladen.
3. Führen Sie das Dienstprogramm aus.

Konfiguration von Gizmo

Bevor Sie beginnen Gizmo zu verwenden, müssen Sie die Anwendung konfigurieren. Wählen Sie **Ansicht >Konfigurieren** und geben Sie die folgenden Parameter ein.



- **KNM Host** – Der DNS-Name oder die IP-Nummer des Computers, der Host für **Network Monitor** ist.
- **Port der WebschnittstelleNetwork Monitor – Die Portnummer, von der aus auf die Verwaltungsschnittstelle von** zugegriffen wird. Standardeinstellungen `8080`.
- **SSL** – Option zur Verbindung mit **Network Monitor** über SSL. Aktivieren Sie diese Option, wenn bei Ihrer **Network Monitor**-Installation SSL für die Verwaltungsschnittstelle verwendet wird.
- **API-Benutzerschlüssel** – Kopieren und fügen Sie Ihren API-Schlüssel aus dem Feld Network Monitor Benutzer > Eigene Einstellungen > Registerkarte "Basiseigenschaften" > **API-Schlüssel** ein. Wenn kein Wert für den API-Schlüssel existiert, klicken Sie auf **Neu** und speichern Sie die Seite **Eigene Einstellungen bearbeiten**.
- **Pfad für Alarmton** – Pfad zu einer `.wav` Datei, die einen Ton enthält, der abgespielt wird, wenn ein Alarm oder Fehler auftritt.
- **Nur Monitorstatus abfragen** – Aktivieren Sie diese Option, wenn der Gizmo ausführende Benutzer keine Administratorrechte für das Windows-Konto hat, um auf die Service-Datenbank und Remoteregistrierung des **Network Monitor**-Hostrechners zuzugreifen.

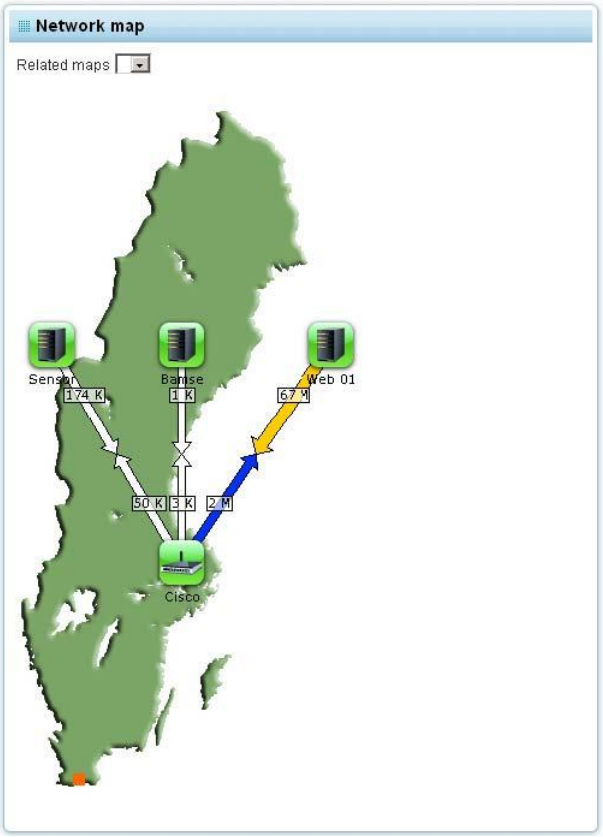
Klicken Sie auf die Schaltfläche **Speichern**, um die Einstellungen zu speichern.

Hinweis: Für das Windows-Konto, das verwendet wird, um Gizmo auszuführen, ist Zugriffsrecht für den Dienststeuerungsmanager des Hostrechners von **Network Monitor** erforderlich. Verwenden Sie **Nur Monitorstatus abfragen**, um diese Anforderung zu umgehen.

Dashboard Map Editor

Network Monitor kann in **Dashboard** *(siehe 92) Netzwerkkarten*-Widgets den Status von Untergruppen und Beständen sowie die Bandbreitenauslastungsdaten anzeigen. Netzwerkkarten werden in der separaten Anwendung **Dashboard Map Editor** (DME) definiert und bearbeitet.

Hinweis: Für das Dienstprogramm **Dashboard Map Editor** ist Microsoft .Net Framework 4.0 oder höher erforderlich.



Starten von Map Editor

Herunterladen und Ausführen von Dashboard Map Editor

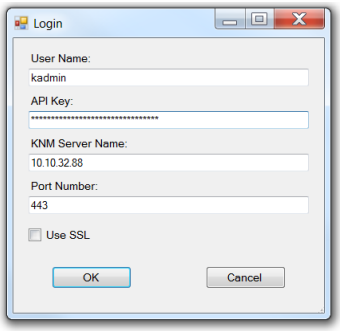
1. Navigieren Sie zur Seite Network Monitor > Werkzeuge > **Downloads Dienstprogramme**.
2. Klicken Sie auf den Link **DME**, um das Dienstprogramm auf den lokalen Rechner herunterzuladen.
3. Führen Sie das Dienstprogramm aus.

Anmelden bei Dashboard Map Editor

Melden Sie sich mit den folgenden Daten bei **Dashboard Map Editor** an:

- **Benutzername** – Ihr VSA-Benutzername.
- **API-Schlüssel** – Ihr API-Schlüssel. Dieser Schlüssel wird mit der Registerkarte Network Monitor > Benutzer > Eigene Einstellungen > **Registerkarte "Basiseigenschaften"** *(siehe 105)* eingerichtet.
- **KNM Servername** – Die Adresse des **Network Monitor**-Servers.

- **Port** – Die zu verwendende Portnummer. Standardeinstellungen `443`.



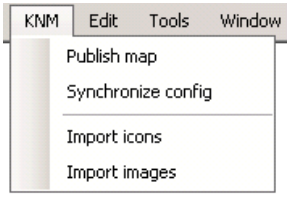
Importieren von Kartenbildern

Importieren von Kartengrafiken

Für die meisten Netzwerkkarten ist es wahrscheinlich sinnvoll, ein Hintergrundbild zu verwenden; beispielsweise ein Bild eines geografischen Standorts oder die Darstellung eines Serverraums. Importieren Sie als erstes das Bild mit dem Editor.

> **Hinweis:** Der Editor unterstützt nur Bilder im Format `.png` (Portable Network Graphics). Wenn Sie ein Bild verwenden wollen, das in einem anderen Format ist, konvertieren Sie dieses mit einer anderen Anwendung.

Um das Bild zu importieren, wählen Sie **Bild importieren** aus dem Menü **KNM**. Wählen Sie dann Ihre Bilddatei aus und klicken Sie auf **OK**. Das Bild wird an den **Network Monitor**-Server gesendet und ist im Editor verfügbar.



Importieren benutzerdefinierter Symbole

Network Monitor bietet eine Reihe vorhandener Symbole, die zur Verwendung mit Netzwerkkarten bereit stehen. Es ist auch möglich eigene benutzerdefinierte Symbole zu importieren, die als Hintergrund für die verschiedenen Entitäten auf Netzwerkkarten verwendet werden können.

> **Hinweis:** Der Editor unterstützt nur Symbole im Format `.png` (Portable Network Graphics). Wenn Sie ein Symbol verwenden wollen, das in einem anderen Format ist, konvertieren Sie dieses mit einer anderen Anwendung.

Um ein benutzerdefiniertes Symbol zu importieren, wählen Sie den Befehl **Symbole importieren** aus dem Menü **KNM** aus. Wählen Sie dann Ihre Bilddatei aus und klicken Sie auf **OK**. Das Bild wird an den **Network Monitor**-Server gesendet und ist im Editor verfügbar.

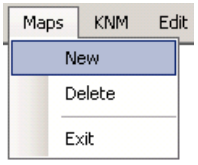
Wenn Ihre Symbole sehr groß sind, funktioniert die Standardmethode für die Statusanzeige im Hintergrund eventuell nicht einwandfrei. In diesen Fällen wird empfohlen, dass Sie die Überlagerungsmethode für den Status verwenden, die im Bereich Netzwerkkarteneinstellungen beschrieben wird.

Hinweis: Es wird empfohlen, um die Bildtransparenz zu gewährleisten, dass die Symbole das 32-Bit-RGBA-Format mit einem eigenen Alphakanal verwenden.

Konfigurieren von Karten

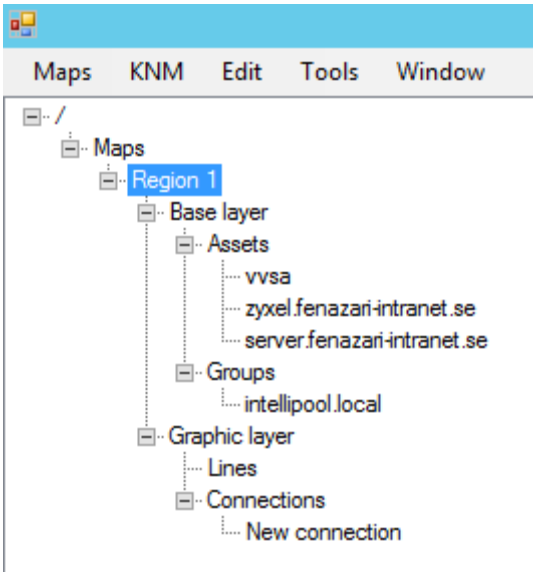
Hinzufügen von Netzwerkkarten

Um eine neue Netzwerkkarte zu erstellen, wählen Sie den Befehl **Neu** aus dem Menü **Karten** aus.



Bearbeiten von Netzwerkkarten

Alle Netzwerkkarten werden als untergeordnete Knoten unter dem **Karten**-Knoten in einer *Kartenstruktur* aufgeführt.



Einstellen von Netzwerkkarteneigenschaften

Klicken Sie auf einen der Netzwerkkartenknoten, um die Basiseigenschaften einzustellen. Nachdem Sie Änderungen in den Karteneigenschaften vorgenommen haben, klicken Sie auf die Schaltfläche **OK**, um die Karte zu aktualisieren.

- **Kartenname** – Der Name der Netzwerkkarte, wie dieser in der Kartenstruktur erscheint. Zum Beispiel: `Region 1`.
- **Kartenbild** – Das für die Karte verwendete Hintergrundbild. Weitere Informationen bezüglich der Vorgehensweise, um Bilder zu importieren, siehe Abschnitt **Importieren von Kartengrafiken** *(siehe 210)*.
- **Hintergrund** – Stellen Sie manuell **Breite**, **Höhe** in Pixeln und die Farbe des **Hintergrunds** der Netzwerkkarte ein.
- **Statuswiedergabe** – Definiert die Art, wie **Network Monitor** den Status von Beständen oder Untergruppen auf der Netzwerkkarte darstellt.
  - `Status in background` – Zeigt den Status als Hintergrund an, wobei das Symbol über die Entität gelegt ist.

- `Status as overlay` – Zeigt das Symbol der Entität mit einem kleinen Statussymbol an, das in der oberen rechten Ecke angefügt ist. Diese Methode wird empfohlen, wenn große benutzerdefinierte Symbole verwendet werden.

Löschen von Netzwerkkarten

Um eine Netzwerkkarte dauerhaft aus **Network Monitor** zu löschen, wählen Sie den Befehl **Löschen** aus dem Menü **Karten**.

Bearbeiten von Kartenknoten

Auswählen von Kartenknoten

Um Inhalt aus der Netzwerkkarte auszuwählen, klicken Sie entweder auf die gewünschte Entität oder ziehen Sie ein Auswahlrechteck um den Inhalt, den Sie auswählen wollen. Der ausgewählte Inhalt wird von einem Rechteck umrahmt angezeigt, um darzustellen, dass er aktuell ausgewählt ist. Um den gesamten Inhalt der Karte auszuwählen, wählen Sie den Befehl **Alle markieren** aus dem Menü **Bearbeiten** oder verwenden Sie die Tastenkombination Strg+A.

- Um Inhalt hinzuzufügen oder Inhalt aus der Auswahl zu löschen, halten Sie die Strg-Taste gedrückt, während Sie auswählen.
- Klicken Sie in einen freien Bereich auf der Karte, um die Auswahl zu löschen.

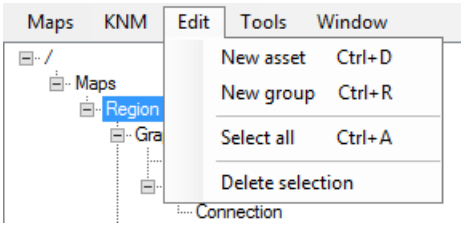
Bearbeiten von Kartenknoten

Um die Eigenschaften des Karteninhalts zu ändern, markieren Sie diesen als erstes, damit das Eigenschaftenfenster erscheint. Führen Sie die entsprechenden (von ihrer Auswahl abhängigen) Änderungen aus und klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu bestätigen.

Um Inhalt auf der Karte zu verschieben, müssen Sie diesen erst auswählen und dann auf der Karte verschieben, während Sie die linke Maustaste gedrückt halten.

Löschen von Kartenknoten

Um Inhalt aus der Karte zu löschen, müssen Sie diesen erst auswählen und anschließend den Befehl **Auswahl löschen** aus dem Menü **Bearbeiten** markieren. Alternativ können Sie die Taste **Löschen** auf der Tastatur drücken.



Mehrfachbearbeitung von Knoten

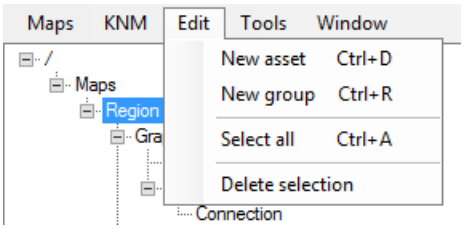
Um in einem Schritt das Symbol zu ändern, das für verschiedene Entitäten verwendet wird, wählen Sie als erstes die entsprechenden Entitäten aus. Wählen Sie dann das gewünschte Symbol im Eigenschaftenbereich aus. Klicken Sie anschließend auf die Schaltfläche **OK**.

Hinzufügen von Kartenknoten

Um der Netzwerkkarte eine **Network Monitor**-Untergruppe oder einen Bestand hinzuzufügen, wählen Sie **Neue Gruppe** oder **Neuer Bestand** aus dem Menü **Bearbeiten** aus.

- Verwenden Sie alternativ die Tastenkombination Strg+N für eine neue Untergruppe.

- Verwenden Sie alternativ die Tastenkombination Strg+O für einen neuen Bestand.



Der Editor platziert eine **Network Monitor**-Untergruppe oder einen Bestand auf eine Standardposition auf der Karte. *Tipp: Wenn die Tastenkombination verwendet wird, wird die neue Untergruppe an der aktuellen Position des Mauscursors platziert.* Die Eigenschaften der Untergruppe oder des Bestands sind im Abschnitt **Eigenschaften** sichtbar.

Die folgenden Eigenschaften können für ausgewählte Untergruppen oder Bestände geändert werden.

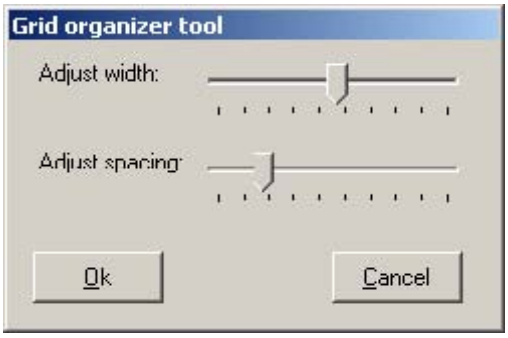
- **Gruppe oder Bestand** – Wählen Sie die **Network Monitor**-Untergruppe oder den Bestand aus, der auf der Karte angezeigt wird.
- **Symbol** – Wählen Sie das Symbol aus, das für die Untergruppe oder den Bestand erscheint. Sie können aus bereits vorhandenen und benutzerdefinierten Symbolen wählen. Siehe Importieren benutzerdefinierter Symbole für weitere Informationen.
- **Position** – Stellen Sie manuell die Position der Untergruppe oder des Bestands ein, indem Sie die x- und y-Koordinaten angeben.
- **Verknüpfungseigenschaften** – Geben Sie an, was passiert, wenn ein Benutzer im **Network Monitor**-Dashboard auf die Untergruppe oder den Bestand klickt.
  - **Keine Verknüpfung** – Es passiert nichts, wenn auf eine Untergruppe oder auf einen Bestand geklickt wird.
  - **Verknüpfung zur Gruppe** – Zeigt die Ansichts-Registerkarten der angegebenen Untergruppe bzw. des Bestands in **Network Monitor** an.
  - **Verknüpfung zur Karte** – Zeigt die angegebene Karte an, wodurch die Erstellung von ''Drilldown'-Karten möglich ist.

Verwenden der Organisationswerkzeuge

Ausgewählter Inhalt der Karte kann mit zwei Werkzeugen geordnet werden: **Werkzeug zur Rastereinordnung** und **Werkzeug zur kreisförmigen Anordnung**. Auf die Werkzeuge greifen Sie zu, indem Sie im Kartenfenster auf die rechte Maustaste klicken, nachdem Sie den gewünschten Inhalt markiert haben und eines der Werkzeuge im Popupmenü **Auswahl ordnen** auswählen.

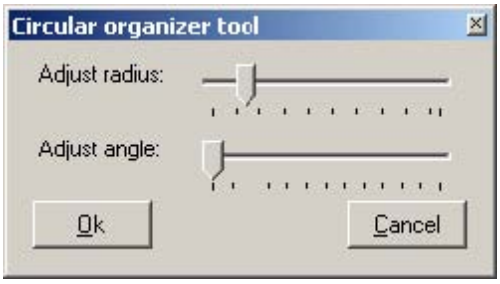
Werkzeug zur Rastereinordnung

Dieses Werkzeug wird verwendet, um die ausgewählten Knoten in einem Raster anzuordnen. Ändern Sie mit den zwei Schiebereglern die Breite des Rasters sowie den Abstand zwischen den einzelnen Entitäten. Änderungen werden sofort in der Karte übernommen.



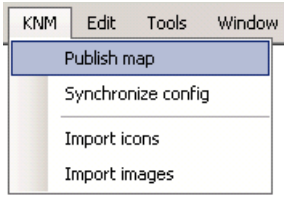
Werkzeug zur kreisförmigen Anordnung

Dieses Werkzeug wird verwendet, um die ausgewählten Entitäten kreisförmig anzuordnen. Ändern Sie mit den zwei Schiebereglern den Radius sowie den Winkel der Entitäten.



Veröffentlichen von Karten

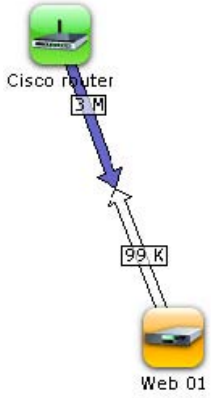
Um Änderungen in einer Netzwerkkarte in **Network Monitor** zu veröffentlichen, wählen Sie den Befehl **Karte veröffentlichen** im Menü **KNM** aus. Die aktuelle Karte wird an den **Network Monitor**-Server gesendet und umgehend aktualisiert.



Visualisierung der Bandbreiten-Auslastung

Network Monitor kann die Bandbreitenauslastung bestimmter Netzwerkschnittstellen direkt und in Echtzeit auf der Netzwerkkarte darstellen. Dieses Merkmal ist ebenfalls für Monitore auf Gateways verfügbar. Auf einer Netzwerkkarte muss eine Verbindung zwischen zwei Knoten angegeben werden, die anschließend mit einem Monitor für `Bandwidth` verknüpft werden muss.

Die visuelle Rückmeldung besteht aus zwei Kreisen, die den eingehend und ausgehenden Datenverkehr der Verbindung darstellen. Der Pfeil für den eingehenden Datenverkehr zeigt auf den Bestand und der Pfeil für ausgehenden Datenverkehr zeigt in die entgegengesetzte Richtung.



Visuelle Rückmeldung der Bandbreitenauslastung

Die Breite und Farbe der Pfeile weisen auf das Auslastungsniveau hin. Je breiter der Pfeil, umso stärker ist die Bandbreitenauslastung.

Die Farbe der Pfeile weist ebenfalls auf das Auslastungsniveau hin. Die Pfeilfarbe geht von weiß (niedrigste Auslastung) über in blau, grün, orange und bis zu rot (höchste Auslastung).

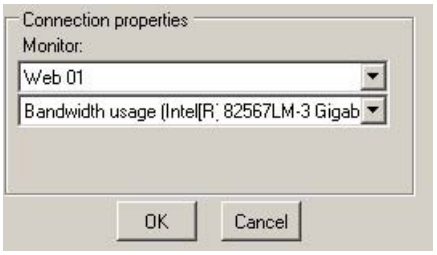
Die Menge des Datenverkehrs, die in jede Richtung geht, ist ebenfalls direkt an der Verbindung sichtbar und wird je nach dem in Kbps/Mbps/Gbps angegeben.

Erstellen einer Bandbreitenverbindung

Die Anzeige der Bandbreitenauslastung auf einer Netzwerkkarte beginnt mit der Erstellung einer Verbindung zwischen zwei Entitäten auf der Karte. Mindestens eine der Entitäten muss ein **Network Monitor**-Bestand sein. Bei der anderen kann es sich um einen anderen Bestand oder eine Untergruppe von **Network Monitor** handeln. Die Verbindung wird dann mit einem bestimmten Monitor für `Bandwidth utilization` in **Network Monitor** verknüpft. Es gibt zwei unterschiedliche Methoden eine Verbindung herzustellen.

Erstellen einer Einzelverbindung

Wählen Sie zwei Knoten auf der Netzwerkkarte aus. Eine muss ein **Network Monitor**-Bestand sein. Klicken Sie dann mit der rechten Maustaste in das Kartenfenster und wählen Sie **Verbindung herstellen** im Popupfenster **Auswahl ändern** aus. Die Verbindung wird linear zwischen den beiden Entitäten hergestellt und so angezeigt. Das Eigenschaftenfenster zeigt die Eigenschaften dieser Verbindung an.

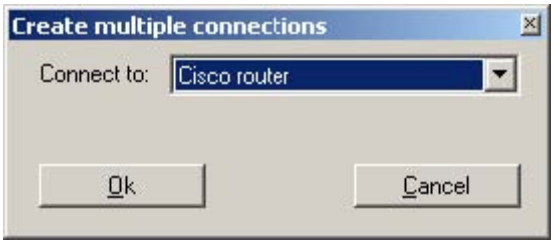


Um die Verbindung mit einem Monitor in **Network Monitor** zu verknüpfen müssen Sie als erstes den Bestand und anschließend den Monitor der Bandbreiten-Auslastung auswählen, dem die Verbindung zugeordnet wird. Der Monitor der Bandbreiten-Auslastung muss bereits für den ausgewählten Bestand definiert sein, damit dieser in der Monitor-Dropdownliste erscheint. Klicken Sie auf die Schaltfläche **OK**, um die Auswahl zu bestätigen.

Sie können optional eine Verbindung herstellen, ohne die Verbindung mit einem Monitor für `Bandwidth utilization` in **Network Monitor** zu verknüpfen. In diesem Fall wird die Verbindung als Linie zwischen den Entitäten auf der Karte angezeigt, wenn diese im Dashboard erscheint, wobei es keine visuellen Informationen zur aktuellen Bandbreitenauslastung gibt.

Erstellen mehrerer Verbindungen

Optional können Sie gleichzeitig mehrere Verbindungen erstellen. Wählen Sie als erstes die gewünschten Knoten auf der Karte aus. Klicken Sie dann mit der rechten Maustaste und wählen Sie **Mehrere Verbindungen herstellen** im Popupfenster **Auswahl ändern** aus.



Wählen Sie den Knoten aus, zu dem mehrere Verbindungen hergestellt werden. Es wird eine neue Verbindung für alle ausgewählten Entitäten erstellt. Der ausgewählte Knoten ist der gemeinsame Endpunkt für jede einzelne Verbindung.

Erstellen einer Verbindung

Klicken Sie zum Bearbeiten einer vorhandenen Verbindung auf die Linie, die die Verbindung in der Kartenansicht darstellt. Die Eigenschaften der ausgewählten Verbindung wird im Eigenschaftenfenster

angezeigt. Um den Monitor der Bandbreiten-Auslastung auszuwählen, der für die Verbindung verwendet wird, wählen Sie als erstes einen relevanten Bestand und anschließend den Monitor der Bandbreiten-Auslastung. Der Monitor der Bandbreiten-Auslastung muss bereits für den ausgewählten Bestand definiert sein, damit dieser in der Monitor-Dropdownliste erscheint. Klicken Sie im Eigenschaftenfenster auf die Schaltfläche **OK**, um die Auswahl zu bestätigen.

Löschen einer Verbindung

Wählen Sie zum Löschen einer Verbindung aus der Karte als erstes diese aus, indem Sie auf die Linie klicken, die die Verbindung in der Kartenansicht darstellt. Die ausgewählte Verbindung wird in der Strukturansicht angezeigt und die Eigenschaften in der Eigenschaftenansicht. Zum Löschen der Verbindung drücken Sie auf die Taste **Löschen** der Tastatur.

Inhaltsverzeichnis

A

Abbilder • 87
Active Directory-Monitor • 117
Aktion "Befehl über SSH2 ausführen" • 156
Aktion "E-Mail senden" • 159
Aktion "Ereignisprotokoll löschen" • 156
Aktion "HTTP Get/Post" • 157
Aktion "Liste zurücksetzen" • 158
Aktion "Lua-Skript" • 159
Aktion "Nachricht über PageGate senden" • 160
Aktion "SMS senden" • 160
Aktion "SNMP-Set" • 161
Aktion "Wake-On-LAN-Paket senden" • 161
Aktion "Windows-Befehl ausführen" • 157
Aktion "Windows-Dienststeuerung" • 163
Aktionsreferenz • 155
Aktivierung des ODBC-Treibers • 185
Alarmmeldungen • 65
Angepasste Datentypen • 106
Anpassen der Firewall-Einstellungen • 199
Anzeigen angepasster Berichte • 73
Anzeigen von Berichtsvorlagen • 70
Arbeitsspeicherverlust bei Remoteregistrierungsdienst auf überwachtem Rechner • 195
Ausfallzeitbericht • 86
Auslagerungsdateiauslastungs-Monitor • 146

B

Backup und Wiederherstellung • 175
Backup von Network Monitor • 175
Bandbreitenauslastungsmonitor • 118
Bearbeiten von Beständen • 49
Bearbeiten von Bestandsvorlagen • 107
Bearbeiten von Gateways • 37
Bearbeiten von Kartenknoten • 212
Bearbeiten von Monitoren • 61
Benutzerarbeitsplan bearbeiten • 95
Benutzerbenachrichtigungsgruppen • 105
Benutzerbenachrichtigungspläne • 95
Benutzerintegration • 28
Berichte • 69
Berichte angepasst • 79
Berichte per E-Mail versenden und veröffentlichen • 73
Berichtsdaten • 82
Berichtsdatentypen • 82
Berichtseigenschaften • 81
Berichtstile • 81
Bestand • 47
Bestandsbefehle und Ansichten • 48
Bestandsvorlagen • 52, 107
Bestandswartung • 93
Bestandswartung bearbeiten • 93
Bestätigen von Alarmen • 68

C

Checkliste vor der Installation • 4
CIM-Monitor • 119
Citrix-Servermonitor • 120
CPU-Auslastungsmonitor • 120

D

Dashboard • 92
Dashboard Map Editor • 208
Dateiänderungsmonitor • 128
Datenansichten • 19
Datenbankservermonitor • 121
Datenextrahierungsreferenz • 176
Datensatzmanagerprotokoll • 100
Datenspeicherauslastung • 122
Datentabellen • 85
Der RPC-Server ist nicht verfügbar • 193
device_xml • 179
devicelist_xml • 181
DHCP-Abfragemonitor • 123
Diagramme • 84
Die Monitoring-Ansicht • 13
Dienstmonitor • 191
dir • 177
DNS-Suchmonitor • 125

E

Eigene Einstellungen • 104
Eigenschaften und Befehle • 20
Eine neue Benutzergruppe erstellen • 105
Ereignis "Befehl über SSH2/Telnet ausführen" • 164
Ereignis "Bericht generieren" • 167
Ereignis "E-Mail senden" • 169
Ereignis "Ereignisprotokoll" löschen • 163
Ereignis "HTTP GET/POST-Anfrage" • 168
Ereignis "Lua-Skripte" • 169
Ereignis "Monitor auslösen" • 172
Ereignis "Nachricht über PageGate senden" • 170
Ereignis "SMS senden" • 170
Ereignis "SNMP-Set" • 171
Ereignis "Statistiken exportieren" • 165
Ereignis "Wake-On-LAN-Paket senden" • 171
Ereignis "Windows-Befehl ausführen" • 164
Ereignis "Windows-Dienststeuerung" • 172
Ereignisprotokollmonitor • 126, 191
Erste Schritte • 13
Erstellen einer Bandbreitenverbindung • 215
Exchange-Servermonitor • 127
Externe Ressourcen • 191

F

Fehlerbehebung • 192
Fehlerbehebung – Windows-Überwachung und -authentifizierung • 190
Formatvariablen • 66

FTP-Servermonitor • 129

G

Gatewaybefehle und -ansichten • 30
Gatewayknoten und Netzwerkermittlung • 25
Gateways • 29
Gizmo • 207
Gruppenbefehle und Ansichten • 44

H

Hinzufügen / Bearbeiten von Untergruppen • 44
Hinzufügen von Kartenknoten • 212
Hinzufügen von Monitoren • 59
Hinzufügen von vorkonfigurierten Monitoren • 60

I

IMAP4-Servermonitor • 129
Importieren von Kartenbildern • 210
Informationen zu Dienstprogrammen • 203
Informationen zum geplanten Ereignis • 163
Informationen zum Navigationsfeld • 77
Init.cfg parameters • 174
Installation • 3
Installieren einer neuen Instanz von Network Monitor R8 • 5
Installieren und Deinstallieren von Gateways • 25
Integration mit Discovery • 23

J

JVM-Systemmonitor • 129

K

Knoten- und Benutzersuche • 16
Knowledge-Base-Artikel • 89
Knowledge-Base-Kategorien • 91
Kommentare • 87
Kompilieren von benutzerdefinierten MIB-Dateien • 99, 204
Konfigurieren von Karten • 211

L

LDAP-Abfragemonitor • 131
Leistungsprobleme bei überwachten Beständen • 193
Liste der Windows-Dienste • 96
Listenansicht filtern • 17
Listenansichten • 15
Listenansichts-Steuerungselemente • 17
Lua • 205
Lua-Skriptmonitor • 132

M

Mailserver-QOS-Monitor • 133
Menüs bearbeiten • 20
MIB Browser • 97
MIB-Objekte • 98
Migration von KNM unabhängig zu KNM integriert • 6
monitor_graph • 177
monitor_status_list • 177
monitor_statusstring • 178
monitor_uptimestring • 178
Monitorbefehle und Ansichten • 55
Monitore • 53
Monitore mit Windows-Authentifizierung • 190
Monitorreferenz • 115
Monitorstruktur • 14
Monitorwartung • 94
MySQL-Monitor • 134

N

Navigationsleiste • 15
Network Monitor -Dienstkonto und Zuweisung von Rechten • 190
Network Monitor Lizensierung in VSA • 28
Network Monitor Modulvoraussetzungen • 4
Network Monitor Überblick • 1
Netzwerkpfad kann nicht gefunden werden • 192
NNTP-Servermonitor • 135
NOC-Einstellungen • 109

O

Oracle-Monitor • 136

P

Pflege überwachen bearbeiten • 94
Ping-Monitor • 137
Planen von Berichten • 75
Plattenauslastungsmonitor • 124
POP3-Servermonitor • 138
Protokolldateimonitor • 131
Protokolleinstellungen • 108
Prozessstatusmonitor • 138

R

Radius-Monitor • 139
Registerkarte "Aktionen" • 56
Registerkarte "Alarm simulieren" • 59
Registerkarte "Alarmfilterung" – Monitore • 64
Registerkarte "Audit" • 37
Registerkarte "Authentifizierung" • 40
Registerkarte "Basiseigenschaften" • 105
Registerkarte "Basiseigenschaften" – Bestand • 50
Registerkarte "Basiseigenschaften" – Gateways • 38
Registerkarte "Basiseigenschaften" – Untergruppen • 45
Registerkarte "Benutzeroberflächenoptionen" • 105
Registerkarte "Bestand" • 31
Registerkarte "Erweitert" – Bestand • 50
Registerkarte "Erweitert" – Gateways • 38
Registerkarte "Erweitert" – Gruppen • 45
Registerkarte "Erweitert" – Monitore • 63
Registerkarte "Grundlegend" – Monitore • 63
Registerkarte "Karte" • 32
Registerkarte "Knowledge" • 37
Registerkarte "Markierungen" • 46
Registerkarte "Monitore" • 32
Registerkarte "Monitoring" • 48
Registerkarte "NOC" • 41
Registerkarte "Statistiken" – Monitore • 64
Registerkarte "Statusänderungsprotokoll" • 49

Registerkarte "Toplist" • 34
Registerkarte "Übersicht" • 56
Registerkarte "Zeitpläne" • 35
Report Templates • 80

S

Salesforce-Abfragemonitor • 140
Schnellberichte anzeigen • 71
Server Sizing • 4
SMS-Einstellungen • 110
SMTP-Servermonitor • 141
SNMP-Monitor • 141
SNMP-Trap-Monitor • 142
So überprüfen Sie, ob KNM Zugriff auf den Remoteregistrierungsdienst hat • 194
Speicherauslastungsmonitor • 133
SQL Server-Monitor • 143
SSH2-Servermonitor • 145
SSH2-Skriptmonitor • 145
Standardnachrichten • 113
Starten von Map Editor • 209
Syslog-Meldung • 101
Syslog-Monitor • 146
System log • 104
Systemadministratorkonsole • 102

T

TCP-Port-Scan-Monitor • 147
Telnet-Servermonitor • 147
Terminaldienstmonitor • 148
test_status • 182
Testen von Abhängigkeiten • 52
TFTP-Servermonitor • 148
Ticket-Aktion • 28, 162
Toplists • 88
Trap-Meldungen • 104

U

Überblick über das Navigationsfeld • 22, 78
Überblick über Dienstprogramme • 204
Überprüfen, ob WMI funktioniert • 199
Überprüfen, ob WMI für das Konto aktiviert ist • 197
Übersicht zur Konfiguration • 9
Übertragungsgeschwindigkeitsmonitor • 148
Umbenennen von Gateways und Beständen • 27
Umgebungsmonitor • 126
UNIX-Systemunterstützungsdateien • 183
Untergruppen • 42
Unternehmen und Rechnergruppen • 26
user_status • 182

V

Vererbung • 15
Veröffentlichen von Karten • 214
Verschieben von Knoten • 21
Version • 183
Verwaltungsschnittstelle • 11
Verwenden der Organisationswerkzeuge • 213
Verzeichniseigenschaftsmonitor • 123
Visualisierung der Bandbreiten-Auslastung • 214
VMware-Systemmonitor • 149
Vollständiger Index von Artikeln zur Fehlerbehebung bei Microsoft WMI • 201
VSA-Integration • 22

W

Webservermonitor • 150
Weitere Systemeinstellungen • 109
Weiterführende Informationen • 173
Wiederherstellen der Konfiguration • 176
Windows-Dienststatusmonitor • 152
Windows-Leistungsregistrierung • 194
Windows-Problembehandlung und -Systemmonitor • 189
Windows-Systemmonitor • 151
Windows-Verwaltungsinstrumentation (WMI) • 195
WMI-Abfragemonitor • 152

Z

Zeitplanblöcke • 96
Zugriff verweigert • 192
Zusatz für Benutzer, die nicht Administrator sind • 199
Zwischenspeichern von Zählern • 195